ADMINISTRATION GUIDE

Cisco Small Business

WAP4410N Wireless-N Access Point
with Power Over Ethernet

OL-19774-01

Contents

About This Document

This guide describes the concepts and tasks necessary to install, configure, and manage the WAP4410N Access Point.

Audience

The audience for this document includes wireless network users, administrators, and managers.

Organization

This table describes the contents of each chapter in this document.

Chapter	Title	Description
Chapter 1	Introduction	Introduces the access point and its capabilities.
Chapter 2	Planning Your Wireless Network	Describes how to connect the access point to the network.
Chapter 3	Getting to Know the Wireless-N Access Point	Describes the physical features of the access point.
Chapter 4	Connecting the WAP4410N Access Point	Explains how to place and connect the access point.
Chapter 5	Setting Up the WAP4410N Wireless-N Access Point	Explains how to use the web-based utility to configure the basic settings of the access point through your web browser.
Chapter 6	Configuring the WAP4410N Wireless-N Access Point	Describes how to configure and manage your WAP4410 access point.

Chapter	Title	Description
Appendix A	Troubleshooting and Help	Provides solutions to problems that may occur during the installation and operation of the access point.
Appendix B	Wireless Security	Discusses security considerations when using a wireless network.
Appendix C	Upgrading Firmware	Provides instructions to upgrade the access point's firmware.
Appendix D	Specifications	Lists the formal specifications of the access point.
Appendix E	Where to Go From Here	Provides links to related sources of information.

Finding Information in PDF Files

The WAP4410N Access Point documents are published as PDF files. The PDF Find/Search tool within Adobe® Reader® lets you find information quickly and easily online. You can perform the following tasks:

- Search an individual PDF file.
- Search multiple PDF files at once (for example, all PDFs in a specific folder or disk drive).
- Perform advanced searches.

Finding Text in a PDF

Follow this procedure to find text in a PDF file.

STEP 1 Enter your search terms in the Find text box on the toolbar.

NOTE By default, the Find tool is available at the right end of the Acrobat toolbar. If the Find tool does not appear, choose **Edit > Find**.

STEP 2 Optionally, click the arrow next to the Find text box to refine your search by choosing special options such as Whole Words Only.

STEP 3 Press **Enter**.

STEP 4 Acrobat displays the first instance of the search term.

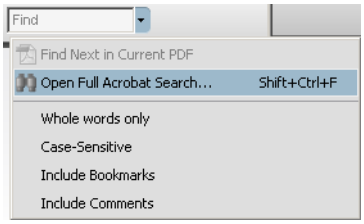
STEP 5 Press **Enter** again to continue to more instances of the term.

Finding Text in Multiple PDF Files

The *Search* window lets you search for terms in multiple PDF files that are stored on your PC or local network. The PDF files do not need to be open.

STEP 1 Start Acrobat Professional or Adobe Reader.

STEP 2 Choose **Edit** > **Search**, or click the arrow next to the *Find* box and then choose **Open Full Acrobat Search**.



STEP 3 In the *Search* window, complete the following steps:

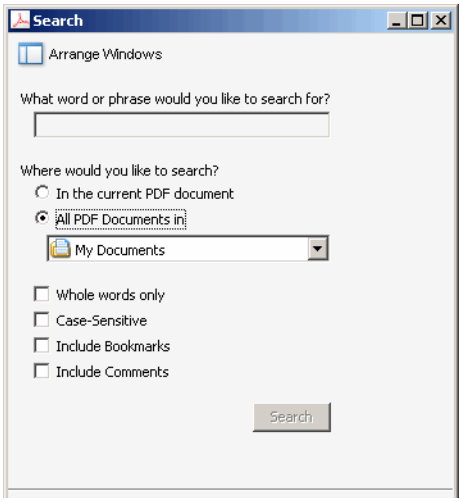
a. Enter the text that you want to find.

b. Choose **All PDF Documents in**.

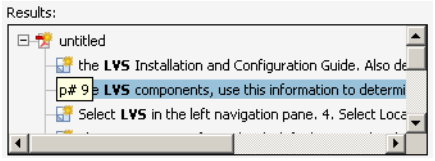
From the drop-down box, choose **Browse for Location**. Then choose the location on your computer or local network, and click **OK**.

c. If you want to specify additional search criteria, click **Use Advanced Search Options**, and choose the options you want.

d. Click **Search**.



STEP 4 When the Results appear, click + to open a folder, and then click any link to open the file where the search terms appear.



For more information about the Find and Search functions, see the Adobe Acrobat online help.

1

Introduction

Thank you for choosing the Cisco WAP4410N Wireless-N Access Point with Power over Ethernet.

This access point allows you to network wirelessly better than ever. An access point allows for greater range and mobility within your wireless network while also allowing you to connect the wireless network to a wired environment.

The Wi-Fi Protected Setup (WPS) feature is also supported to help you simplify the setting up and configure security on a wireless network.

The Cisco WAP4410N Wireless-N Access Point with Power over Ethernet even offers the convenience of Power over Ethernet (PoE) capability (in addition to regular 12VDC power adaptor), so it can receive data and power over a single Ethernet network cable.

The WAP4410N Access Point supports the 802.11n Draft 2.0 Specification by IEEE. It also support 802.11g and 802.11b clients in a mixed environment. This access point can support 802.11n connections, which are much faster than the earlier 802.11b/g technologies. In addition, this access point provides longer coverage by using multiple antennas to transmit and receive data streams in different directions.

Networks are useful tools for sharing computer resources. You can access one printer from different computers and access data located on another computer's hard drive. Networks are even used for playing multiplayer video games. So, networks are not only useful in homes and offices, they can also be fun.

Computers on a wired network create a LAN, or Local Area Network. They are connected with Ethernet cables, which is why the network is called “wired.”

Computers equipped with wireless client cards or adapters can communicate without cumbersome cables. By sharing the same wireless settings within their transmission radius, they form a wireless network.

This is sometimes called a WLAN, or Wireless Local Area Network. The access point bridges wireless networks of 802.11n, 802.11g and 802.11b standards and wired networks.

1

Use the instructions in this guide to help you connect the access point, set it up, and configure it to bridge your different networks. These instructions should be all you need to get the most out of the access point.

2

Planning Your Wireless Network

Network Topology

A wireless network is a group of computers, each equipped with one or more wireless adapters. Computers in a wireless network must be configured to share the same radio channel to talk to each other. Several computers equipped with wireless cards or adapters can communicate with each other to form an ad-hoc network without the use of an access point.

Cisco also provides products to allow wireless adaptors to access wired network through a bridge such as the wireless access point, or wireless router. An integrated wireless and wired network is called an infrastructure network. Each wireless computer in an infrastructure network can talk to any computer in a wired or wireless network via the access point or wireless router.

An infrastructure configuration extends the accessibility of a wireless computer to a wired network, and may double the effective wireless transmission range for two wireless adapter computers. Since an access point is able to forward data within a network, the effective transmission range in an infrastructure network may be more than doubled since access point can transmit signal at higher power to the wireless space.

Roaming

Infrastructure mode also supports roaming capabilities for mobile users. Roaming means that you can move your wireless computer within your network and the access points will pick up the wireless computer's signal, providing that they both share the same wireless network (SSID) and wireless security settings.

Before you consider roaming, choose a feasible radio channel and optimum access point position. Proper access point positioning combined with a clear radio signal will greatly enhance performance.

Network Layout

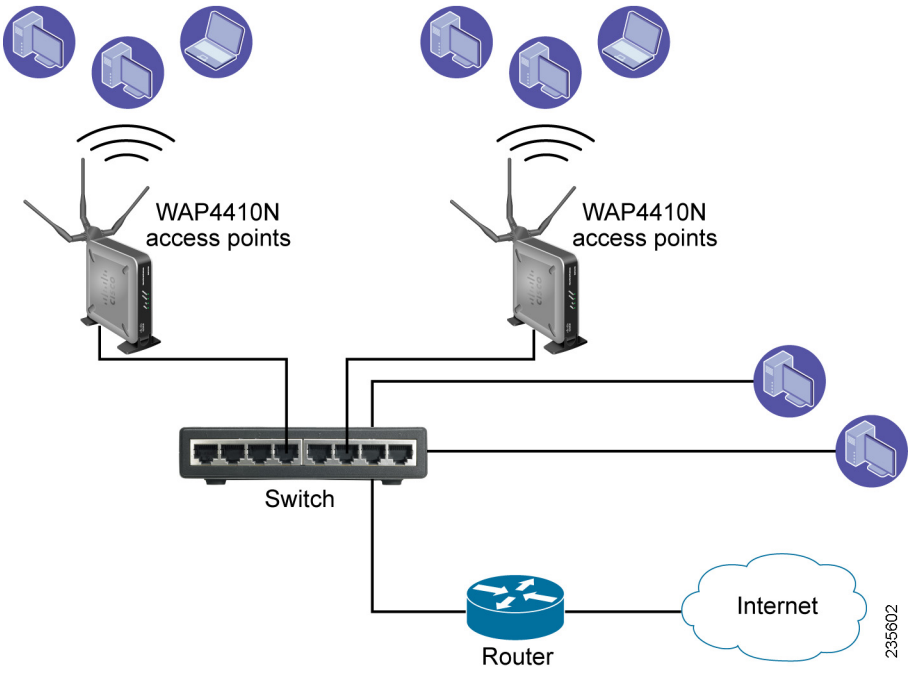
The Wireless-N Access Point has been designed for use with 802.11n, 802.11g and 802.11b products. The access point is compatible with 802.11n, 802.11g and 802.11b adapters, such as the notebook adapters for your laptop computers, PCI adapters for your desktop PCs, and USB adapters for all PCs when you want to enjoy wireless connectivity. These wireless products can also communicate with a 802.11n, 802.11g or 802.11b wireless print server (if available).

To link your wired network with your wireless network, connect the access point's Ethernet network port to any switch or router with Power over Ethernet (PoE)—or a PoE injector, such as the Cisco WAPPOE or WAPPOE12. Note that the 12 VDC on the WAPPOE12 is for the splitter output.

With these, and many other, Cisco products, your networking options are limitless. Go to the Cisco website at www.cisco.com for more information about wireless products.

Example of a Simple Wireless Network

The diagram below shows a typical infrastructure wireless network setup.



The wireless access points are connecting to a Cisco switch that provides them with power. Each access point can connect multiple wireless devices to the network.

This network provides connectivity among wireless network devices and computers that have a wired connection to the switch.

The switch connects to a router that connects to the Internet.

3

Getting to Know the Wireless-N Access Point

This chapter describes the external features of the WAP4410N Access Point.

Front Panel

The access point's front panel LEDs display information about network activity.

POWER LED—(Green) Lights up and remains lit when the device is powered on.

PoE LED—(Green) Lights up when the access point is powered through an Ethernet cable.

WIRELESS LED—(Green) Lights up when the wireless module is active on the access point. This LED flashes when the access point is actively sending to or receiving data from a wireless device.

ETHERNET LED—(Green) Lights up when the access point successfully connects to a device through the Ethernet network port. This LED flashes when the access point is actively sending to or receiving data from one of the devices over the Ethernet network port.

Back Panel

The ports of the access point are located on the back panel of the switch.

RESET Button—There are two ways to reset the access point to the factory default configuration. Either press the Reset button for approximately 10 seconds or restore the defaults using the web-based utility of the access point.

ETHERNET Port—Connects to Ethernet network devices, such as a switch or router that may or may not support PoE.

POWER Port—Connects the access point to power using the supplied 12VDC power adapter.

Antennas and Positions

The WAP4410N Access Point has three detachable 2dBi omni-directional antennas. These antennas are located on the back of the device.

The three antennas have a base that can rotate 90 degrees when in the standing position. The three antennas support 3X3 “multiple in, multiple out” (MIMO) diversity in wireless-N mode.

4

Connecting the WAP4410N Access Point

This chapter describes how to place and connect the WAP4410N Access Point to your network.

Depending on your application, you might want to set up the device first before mounting it.

Placement Options

You can place the WAP4410N Access Point horizontally on its rubber feet, vertically in a stand, or mount it on the wall.

Desktop Option

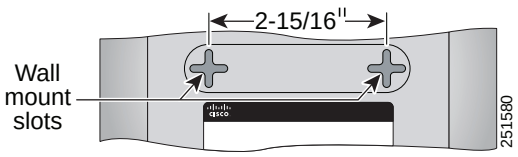
For desktop mounting, place the access point horizontally on a surface so it sits on its four rubber feet.

Wall-Mount Option

To mount the WAP4410N Access Point on a wall, follow these steps.

STEP 1 Determine where you want to mount the WAP4410N Access Point and install two screws (not supplied) that are 2-15/16 inches apart (approximately 7.46 cm.).

STEP 2 With the back panel pointing up (if installing vertically), line up the WAP4410N Access Point so that the wall-mount crisscross slots on the bottom of the access point line up with the two screws.



STEP 3 Place the wall-mount slots over the screws and slide the WAP4410N Access Point down until the screws fit snugly into the wall-mount slots.

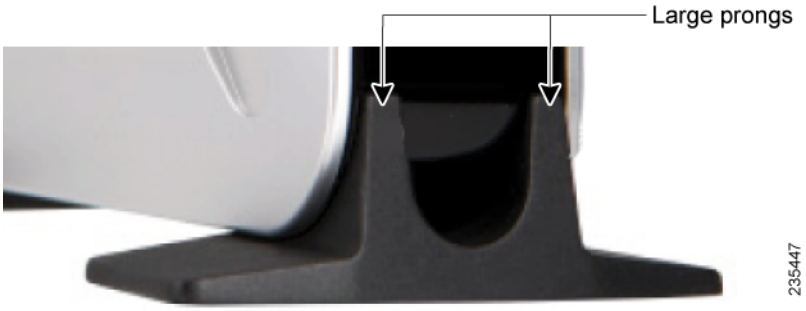
Stand Option

To place the access point vertically in a stand, follow these steps.

STEP 1 Locate the left side panel of the WAP4410N Access Point.

STEP 2 With the two large prongs of one of the stands facing outward, insert the short prongs into the little slots in the WAP4410N Access Point, and push the stand upward until the stand snaps into place.

Repeat this step with the other stand.



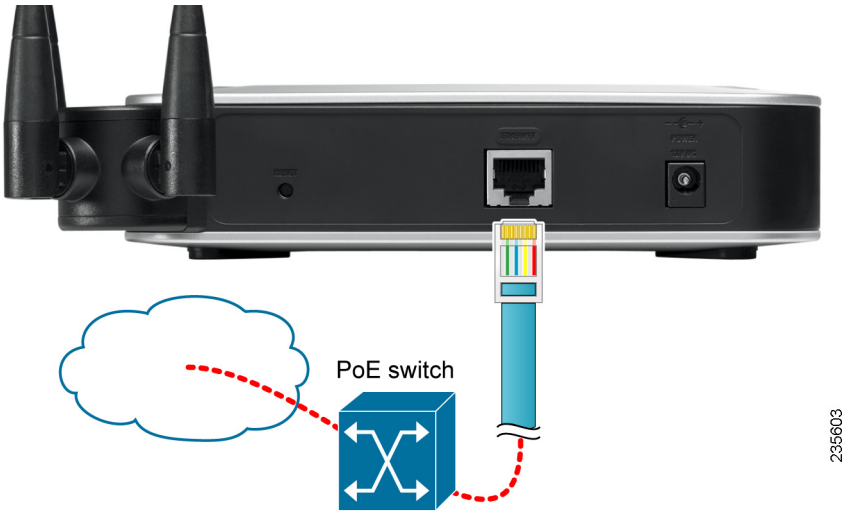
Connecting the WAP4410N Access Point to the Network

You can connect the WAP4410N Access Point to your network in one of the following ways:

- Using a PoE switch
- Using a standard switch

Using a PoE Switch to Connect the WAP4410N Access Point to the Network

To connect the WAP4410N Access Point to your network using a PoE switch, simply connect the Ethernet port of the access point to a PoE port on the PoE switch.



The LEDs on the front panel light up as soon as the WAP4410N Access Point powers on.

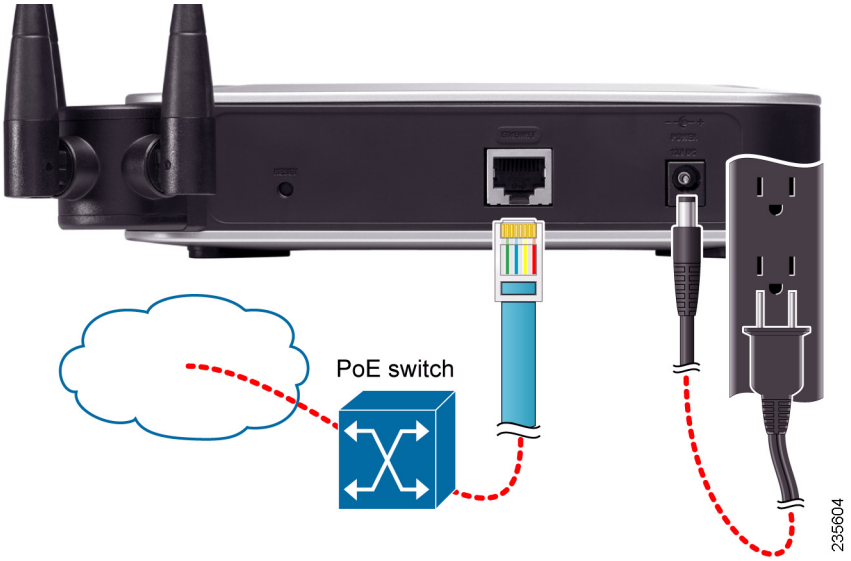
Using a Standard Switch to Connect the WAP4410N Access Point to the Network

To connect the WAP4410N Access Point to your network using a standard switch, follow these steps.

STEP 1 Use the supplied Ethernet cable to connect the Ethernet port of the access point to an Ethernet port on the switch.

STEP 2 Connect the included power adapter to the Power port of the WAP4410N Access Point.

STEP 3 Plug the power adapter into an electrical outlet.



The LEDs on the front panel light up as soon as the WAP4410N Access Point powers on.

5

Setting Up the WAP4410N Wireless-N Access Point

The WAP4410N Access Point works right out of the box with the default settings. However, you can change these settings to suit your needs by accessing the access point using a web-based configuration utility.

NOTE: Make sure you have Enabled TCP/IP on your computers prior to proceeding. Computers communicate over the network with this protocol.

Launching the Web-Based Configuration Utility

To configure the WAP4410N Access Point, follow these steps to access the WAP4410N web-based configuration utility from your computer.

STEP 1 Connect your computer to the same network the WAP4410N Access Point is connected to.

STEP 2 Configure your computer to be on the same subnet as the access point (for example 192.168.1.199).

By default, the WAP4410N Access Point has an IP address of 192.168.1.245 and a default mask of 255.255.255.0.

STEP 3 Launch a web browser, such as Internet Explorer or Mozilla Firefox.

STEP 4 In the Address field enter **192.168.1.245** and press the **Enter** key.

STEP 5 In the User Name and Password fields enter **admin**.

The default user name and password is **admin**.

STEP 6 Click **Log in**.

Navigating the Utility

The web-based utility consists of the following main screens:

- Setup
- Wireless
- Security Monitor
- Administration
- Status

Setup

This screen allows you to configure the host name and IP address settings and to set the time. This screen consists of the following screens:

- **Basic Setup**—Configures the host name and IP address settings for this access point.
- **Time**—Sets the time on this access point.
- **Advanced**—Sets the HTTP Redirect and 802.1x supplicant settings for this access point.

Wireless

This screen allows you to enter a variety of wireless settings for the access point.

- **Basic Wireless Settings**—Configures the wireless network mode (for example, B/G/N-Mixed), SSID, and radio channel.
- **Wireless Security**—Configures the access point's security settings.
- **Wireless Connection Control**—Controls the wireless connections from client devices to this access point.
- **Wi-Fi Protected Setup**—Simplifies the process of setting up and configuring security on a wireless network.

- **VLAN & QoS**—Configures the 802.1Q VLAN and the Quality of Service (QoS) settings.
- **Advanced Wireless Settings**—Configures the access point's more advanced wireless settings (for example, load balancing and channel bandwidth).

AP Mode

This screen allows you to select the mode of operation for the access point. The default mode is Access Point.

Administration

This screen allows you to manage the access point.

- **Management**—Configures the password and Simple Network Management Protocol (SNMP) settings.
- **Log**—Configures the log settings.
- **Diagnostic**—Allows you to perform diagnostic activities, which can be useful in solving network problems.
- **Factory Default**—Resets the access point to its factory default settings.
- **Firmware Upgrade**—Upgrades the access point's firmware on this screen.
- **Reboot**—Reboots the access point.
- **Config Management**—Saves and restores access point configuration.

Status

This screen allows you to view status information about your local network, wireless networks, and network performance.

- **Local Network**—Displays system information, including software and hardware versions, MAC address, and IP address on the LAN side of the access point.
- **Wireless**—Displays wireless network settings including SSID, network mode, priority setting, VLAN trunk, and wireless channel.

- **System Performance**—Displays the current traffic statistics of this access point for both wireless and LAN ports.

6

Configuring the WAP4410N Wireless-N Access Point

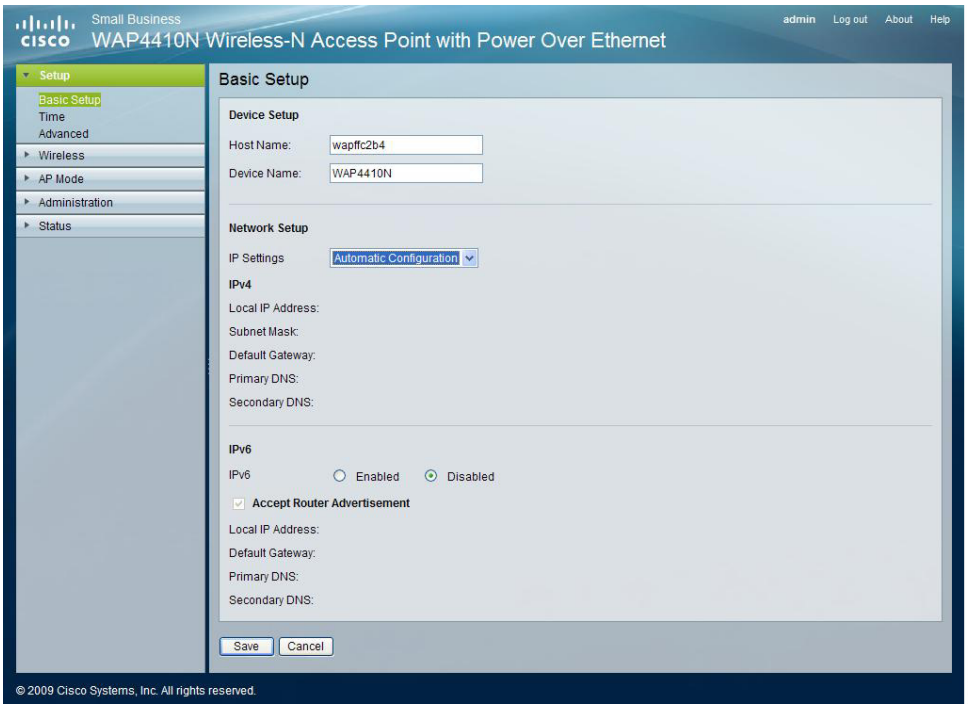
This chapter describes how to configure your WAP4410N Access Point using the web-based configuration utility.

Setting Up Your Access Point

This section describes how to configure the general settings of the access point:

Configuring Basic Setup Settings

The Setup > Basic Setup page displays the general settings of the access point.



You can configure the following basic setup settings:

- "Configuring Device Setup Settings" on page 20
- "Configuring Network Setup Settings" on page 20

Configuring Device Setup Settings

To configure the device setup settings of the access point, follow these steps:

STEP 1 Click **Setup > Basic Setup**.

STEP 2 In the Device Setup section, enter the following information:

- **Host Name**—Enter the host name of the access point.

  You can use the host name to access the web-based configuration utility through the network if a record of the host name exists in your DNS server.

  The access point publishes the host name to your DNS server if you configured the access point to acquire its IP address from a DHCP server.

  Follow your organization's policy when assigning this name.

  The default name is **Cisco**.

- **Device Name**—Enter the device name for the access point.

  This name is identification purposes only. Unique, memorable names are helpful, especially if you are deploying multiple access points on the same network. This name helps you identify the access point after you log in.

  The default name is **WAP4410N**.

STEP 3 Click **Save**.

Configuring Network Setup Settings

To configure the network setup settings of the access point, follow these steps:

STEP 1 Click **Setup** > **Basic Setup**.

STEP 2 From the **IP Settings** drop-down menu, select one of the following options:

- **Static IP Address**—Select this option to assign a static or fixed IP address to the access point.
- **Automatic Configuration**—Select this option to automatically configure the IPv4 network settings of the access point using a DHCP server on your network. Also select this option to automatically configure the IPv6 network settings of the access point using an IPv6 RADVD device enabled on your network.

STEP 3 If you select **Static IP Address** from the **IP Settings** drop-down menu, enter the following information in the IP4V section of the screen:

- **IP Address**—Enter a unique IP address for your access point. The default IP address is **192.168.1.245**.
- **Subnet Mask**—Enter the same subnet mask used in your network. The default is **255.255.255.0**.
- **Default Gateway**—Enter the IP address of your Gateway or Router. Enter the value used by other devices on your LAN.
- **Primary DNS**—Enter the IP address of your primary DNS server.
- **Secondary DNS**—Enter the IP address of your secondary DNS server.

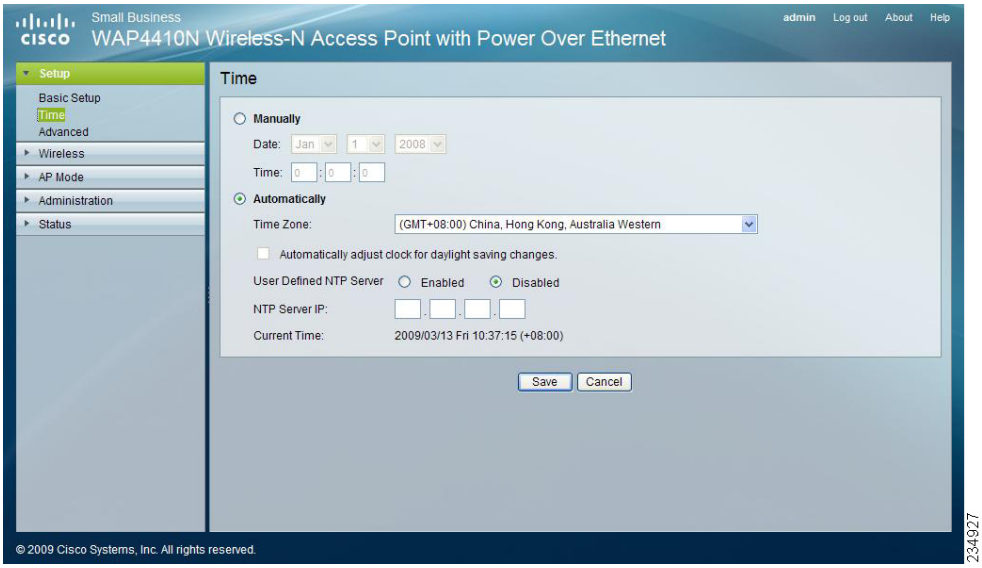
STEP 4 To configure the IPv6 settings for your access point:

- **IPv6**—Select Enabled to enable IPv6 for your access point.
- **Accept Router Advertisement**—Check this check box to accept router advertisement.
- **Local IP Address**—Enter a unique IP address for your access point.
- **Default Gateway**—Enter the IP address of your gateway or router. This address is used by the other devices on your network.
- **Primary DNS**—Enter the IP address of your primary DNS server.
- **Secondary DNS**—Enter the IP address of your secondary DNS server.

STEP 5 Click **Save**.

Configuring Time Settings

The Time screen displays the time settings of the access point. By setting up the correct time, you can help your network administrator search the system log to identify problems.



To configure the time settings for the access point, follow these steps:

STEP 1 Click **Setup** > **Time**.

STEP 2 To manually configure the time settings:

a. Select **Manually**.

b. In the **Date** field enter the date.

c. In the **Time** field enter the time.

STEP 3 To automatically configure the time settings to obtain the time from a time server on your network or on the Internet:

a. Select **Automatically**.

b. From the **Time Zone** drop-down menu, select a time zone.

c. If appropriate, check the **Automatically adjust clock for Daylight Saving changes** check box.

d. To get the time from a local NTP server, in the User Defined NTP Server field, click Enabled.

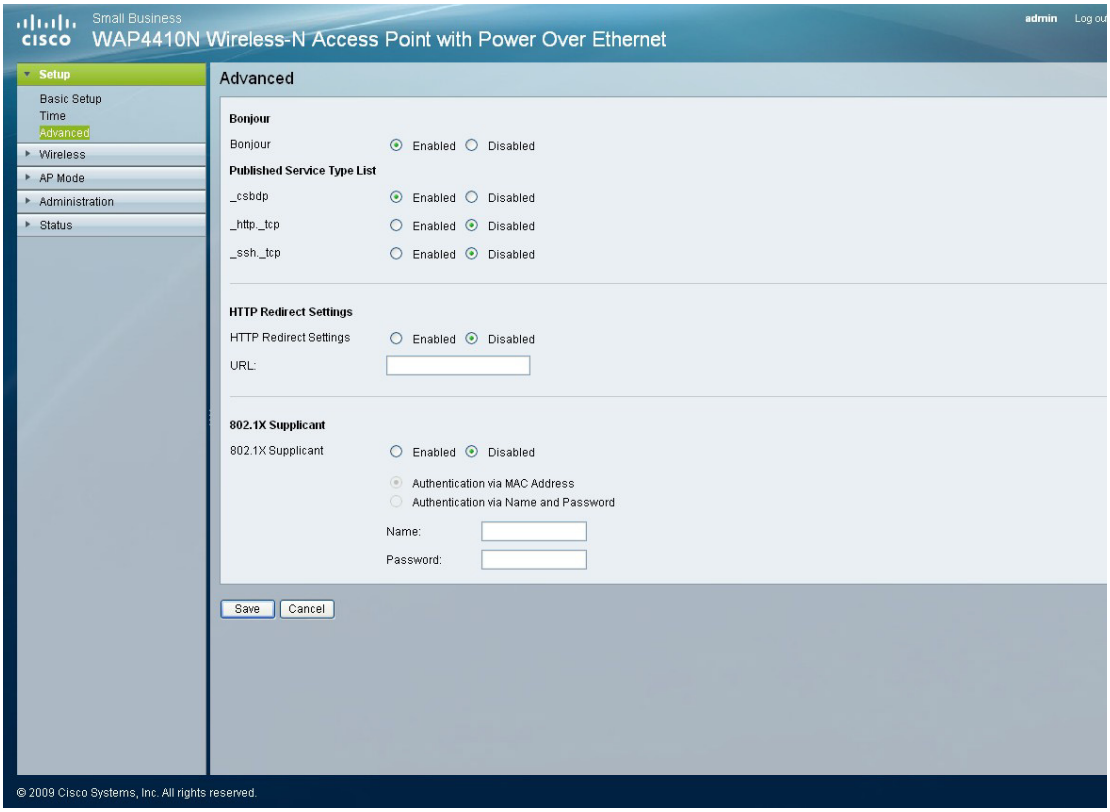
e. In the **NTP Server IP** field, enter the IP address of the NTP server.

- **User Defined NTP Server**—Enable this option if you have set up local NTP server. Default is **Disabled**.
- **NTP Server IP**—Enter the IP address of user defined NTP Server.

STEP 4 Click **Save**.

Configuring Advanced Settings

The Setup > Advanced Settings page displays advanced settings.



To configure the advanced setup settings of the access point, follow these steps:

STEP 1 Click **Setup > Advanced**.

STEP 2 To enable Bonjour, click **Enabled**.

STEP 3 To enable HTTP redirect settings:

a. In the HTTP Redirect Settings field, click **Enabled**.

b. In the URL field, enter the URL to redirect the HTTP settings to.

STEP 4 To enable 802.1X supplicant settings:

a. In the 802.1x Supplicant field, click **Enabled**.

b. To use the MAC address for authentication, click **Authentication via MAC Address**.

c. To use a name and password for authentication, click **Authentication via Name and Password** and enter the name and password in the corresponding fields.

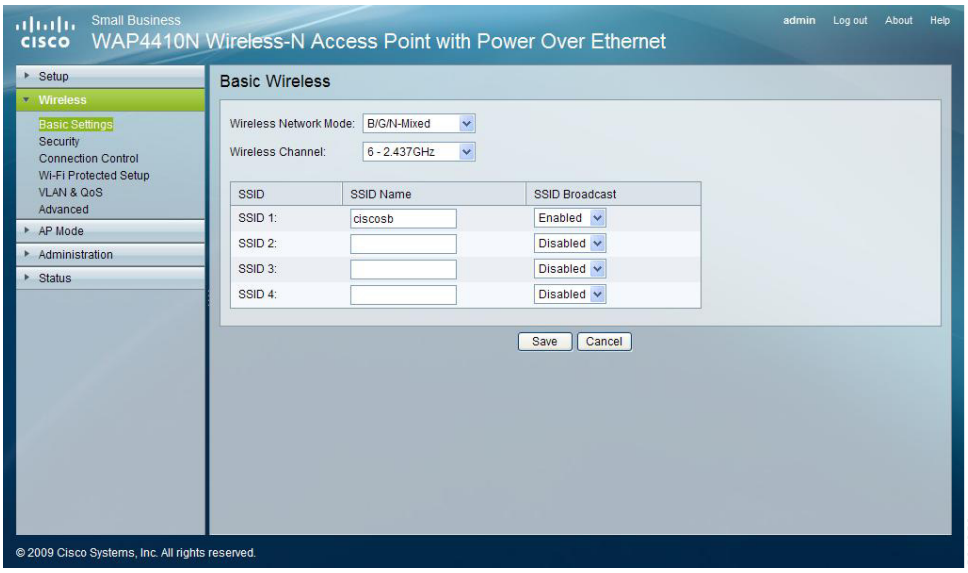
STEP 5 Click **Save**.

Wireless

This section describes how to configure the wireless settings of the access point:

Configuring Basic Settings

The Wireless > Basic Settings page displays the basic wireless network settings.



To configure the basic attributes for this access point, follow these steps:

STEP 1 Click **Wireless > Basic Settings**.

STEP 2 From the Wireless Network Mode field, select one of the following modes:

- **Disabled**—Disables wireless connectivity completely. This might be useful during system maintenance.
- **B-Only**—Connects all the wireless client devices to the access point at Wireless-B data rates with maximum speed at 11 Mbps.
- **G-Only**—Connects both Wireless-N and Wireless-G client devices at Wireless-G data rates with maximum speed at 54Mbps. Wireless-B clients cannot be connected in this mode.
- **N-Only**—Connects only Wireless-N client devices at Wireless-N data rates with maximum speed at 300 Mbps.
- **B/G-Mixed**—Connects both Wireless-B and Wireless-G client devices at their respective data rates. Wireless-N devices can be connected at Wireless-G data rates.
- **B/G/N-Mixed**—(Default) Connects all the wireless client devices at their respective data rates in this mixed mode.

STEP 3 From the Wireless Channel drop-down menu, select the appropriate channel to be used among your access point and client devices.

The default is channel 6.

You can also select **Auto** from the Wireless Channel drop-down menu so that your access point selects the channel with the lowest amount of wireless interference while the system is powering up.

Automatic channel selection starts when you click **Save**. It takes several seconds to scan through all the channels to find the best channel.

For the Wireless-N 40MHz channel option (see the Wireless > Advanced screen), the access point automatically selects the adjacent 20 MHz channel to combine them into a wider channel.

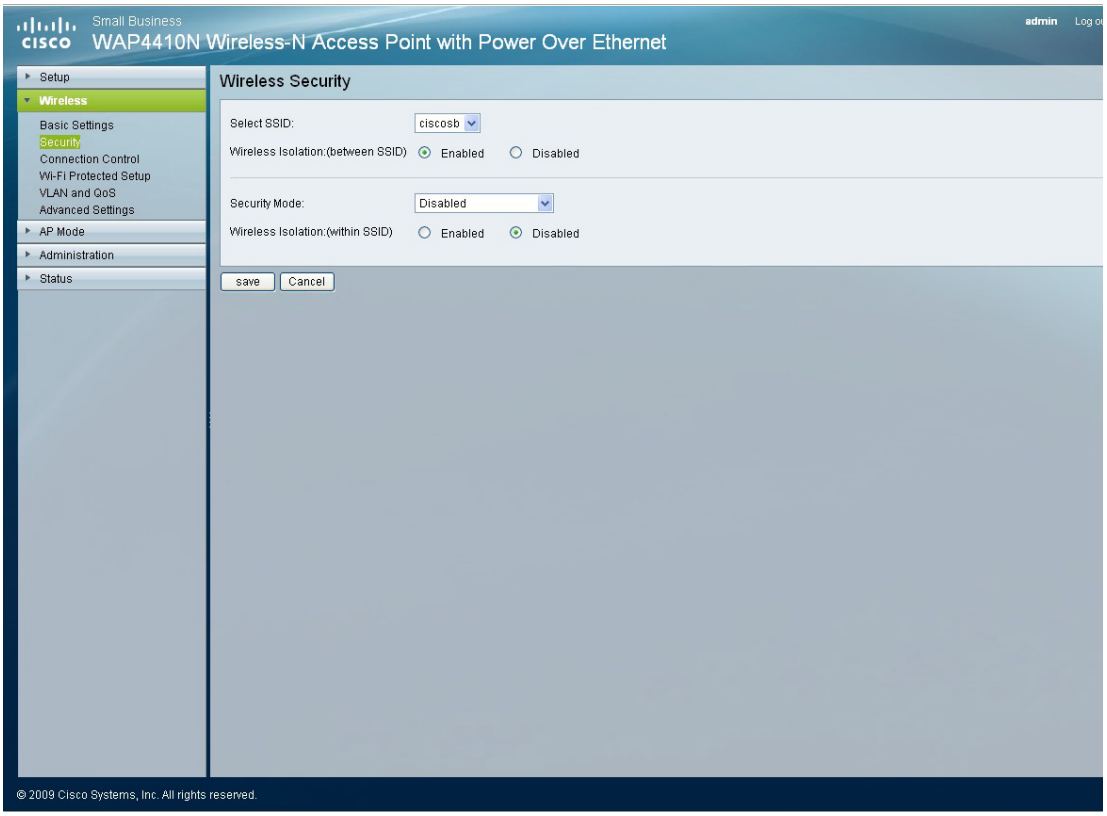
STEP 4 In the **SSID Name** and **SSID Broadcast** fields, enter the SSIDs you want your access point to broadcast:

- **SSID Name**—This field specifies a unique SSID that is shared among all devices in a wireless network. It is case-sensitive, must not exceed 32 alphanumeric characters, and may contain any keyboard character. Make sure this name is used by all devices in your wireless network. The default SSID name is **ciscosb**.
- **SSID Broadcast**—Allows the SSID to be broadcast on your network. You might want to enable this function while configuring your network, but make sure that you disable it when you are finished. With this option enabled, someone can easily obtain the SSID information with site survey software or Windows XP and gain unauthorized access to your network. Select **Enabled** to broadcast the SSID to all wireless devices in range. Select **Disabled** to increase network security and prevent the SSID from being seen on networked PCs. The default is **Enabled** in order to help users configure their network before using it.

STEP 5 Click **Save**.

Configuring Security

The Wireless > Security page displays the wireless security settings of the access point.



To configure the wireless security settings of the access point, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 To configure wireless isolation between SSIDs:

a. From the **Select SSID** drop-down menu select an SSID.

b. To isolate wireless clients from each other, click **Enabled**. Otherwise, click **Disabled**.

STEP 3 To disable wireless security completely, from the Security Modes drop-down, select **Disabled**.

This is the default setting.

STEP 4 To enable wireless security, from the Security Mode drop-down menu, select one of the following security modes and provide the required information, as described in the sections below.

- **WPA-Personal**
- **WPA2-Personal**
- **WPA2-Personal Mixed**
- **WPA-Enterprise**
- **WPA2-Enterprise**
- **WPA2-Enterprise Mixed**
- **Radius**
- **WEP**

STEP 5 To prevent wireless computers associated to the same SSID from seeing and transferring files between each other, in the Wireless Isolation (within SSID) field, click **Enabled.**

This feature is very useful when setting up a wireless hotspot location. The default is Disabled.

STEP 6 Click **Save.**

Configuring WAP-Personal Security

Wi-Fi Protected Access (WPA) Personal (WAP-Personal) is a security standard stronger than WEP encryption and forward compatible with IEEE 802.11e. WPA-Personal is also known as WAP-PSK.

To enable wireless WPA-Personal security, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 From the Security Mode drop-down menu, select **WAP-Personal**.

STEP 3 To enable wireless isolation within the SSID, click **Enabled**.

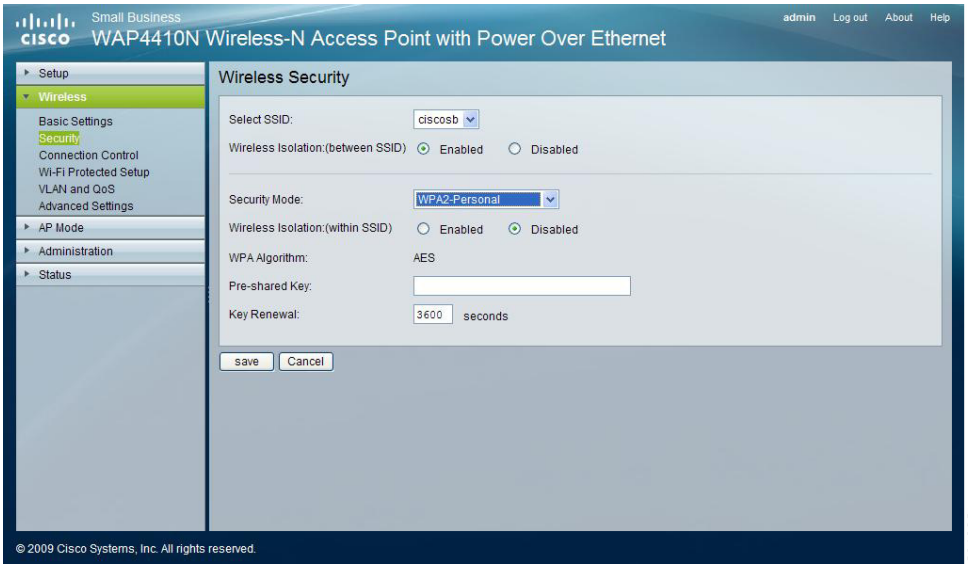
STEP 4 Provide the following information:

- **WPA Algorithms**—WPA offers you two encryption methods, TKIP and AES for data encryption. Select the type of algorithm you want to use, **TKIP** or **AES**. The default is **TKIP**.
- **Pre-Shared Key**—Enter a WPA Shared Key of 8–63 characters.
- **Key Renewal**— Enter a key renewal timeout period, which instructs the access point how often it should change the encryption keys. The default is **3600** seconds.

STEP 5 Click **Save**.

Configuring WAP2-Personal Security

This security mode supports the WPA2-Personal protocol.



To enable wireless WPA2-Personal security, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 From the Security Mode drop-down menu, select WAP2-Personal.

STEP 3 To enable wireless isolation within the SSID, click **Enabled**.

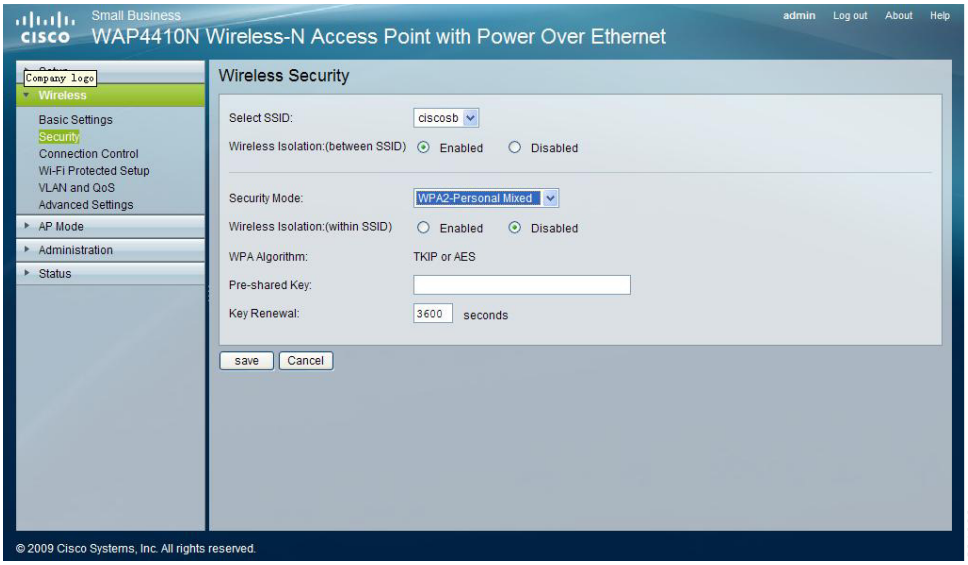
STEP 4 Provide the following information:

- **WPA Algorithms**—(Read-only) WPA2-Personal automatically chooses AES for data encryption.
- **Pre-Shared Key**—Enter a WPA Shared Key of 8–63 characters.
- **Key Renewal**—Enter a key renewal timeout period, which instructs the access point how often it should change the encryption keys. The default is **3600** seconds.

STEP 5 Click **Save**.

Configuring WPA2-Personal Mixed Security

This security mode supports the transition from WPA-Personal to WPA2-Personal. You can have client devices that use either WPA-Personal or WPA2-Personal. The access point will automatically choose the encryption algorithm used by each client device.



To enable wireless WPA2-Personal Mixed security, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 From the Security Mode drop-down menu, select WPA2-Personal Mixed.

STEP 3 To enable wireless isolation within the SSID, click **Enabled**.

STEP 4 Provide the following information:

- **WPA Algorithms**—(Read-only) The WPA2-Personal Mixed security mode automatically chooses TKIP or AES for data encryption.
- **Pre-Shared Key**—Enter a WPA Shared Key of 8–63 characters.
- **Key Renewal**— Enter a key renewal timeout period, which instructs the access point how often it should change the encryption keys. The default is **3600** seconds.

STEP 5 Click **Save**.

Configuring WPA-Enterprise Security

The WPA-Enterprise mode features WPA used in coordination with a RADIUS server for client authentication.

CAUTION Use this mode only when a RADIUS server is connected to the access point.

To enable wireless WPA-Enterprise security, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 From the Security Mode drop-down menu, select WPA-Enterprise.

STEP 3 To enable wireless isolation within the SSID, click **Enabled**.

STEP 4 Provide the following information:

- **Primary/Backup RADIUS Server**—Enter the IP address of the RADIUS server. The Backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The backup Radius server is used only if the primary server is unavailable.

- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the access point and RADIUS server. The backup Radius server is used only if the primary server is unavailable.
- **WPA Algorithms**—WPA offers two encryption methods, TKIP and AES for data encryption. Select one of these algorithms from the drop-down menu. The default is **TKIP**.
- **Key Renewal Timeout**—Enter a key renewal timeout period, which instructs the access point how often it should change the encryption keys. The default is **3600** seconds.

STEP 5 Click **Save**.

Configuring WPA2-Enterprise Security

The WPA2-Enterprise mode features WPA2 used in coordination with a RADIUS server for client authentication.

CAUTION Use this mode only when a RADIUS server is connected to the access point.

To enable wireless WPA2-Enterprise security, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 From the Security Mode drop-down menu, select WPA2-Enterprise.

STEP 3 To enable wireless isolation within the SSID, click **Enabled**.

STEP 4 Provide the following information:

- **Primary/Backup RADIUS Server**—Enter the IP address of the RADIUS server. The Backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the access point and RADIUS server. The backup Radius server is used only if the primary server is unavailable.
- **WPA Algorithms**—WPA2 always uses AES for data encryption.
- **Key Renewal Timeout**—Enter a key renewal timeout period, which instructs the access point how often it should change the encryption keys. The default is **3600** seconds.

STEP 5 Click **Save**.

Configuring WPA2-Enterprise Mixed Security

This security mode supports the transition from WPA-Enterprise to WPA2-Enterprise. You can have client devices that use either WPA-Enterprise or WPA2-Enterprise. The access point will automatically choose the encryption algorithm used by each client device.

CAUTION Use this mode only when a RADIUS server is connected to the access point.

To enable wireless WPA2-Enterprise Mixed security, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 From the Security Mode drop-down menu, select WPA2-Enterprise Mixed.

STEP 3 To enable wireless isolation within the SSID, click **Enabled**.

STEP 4 Provide the following information:

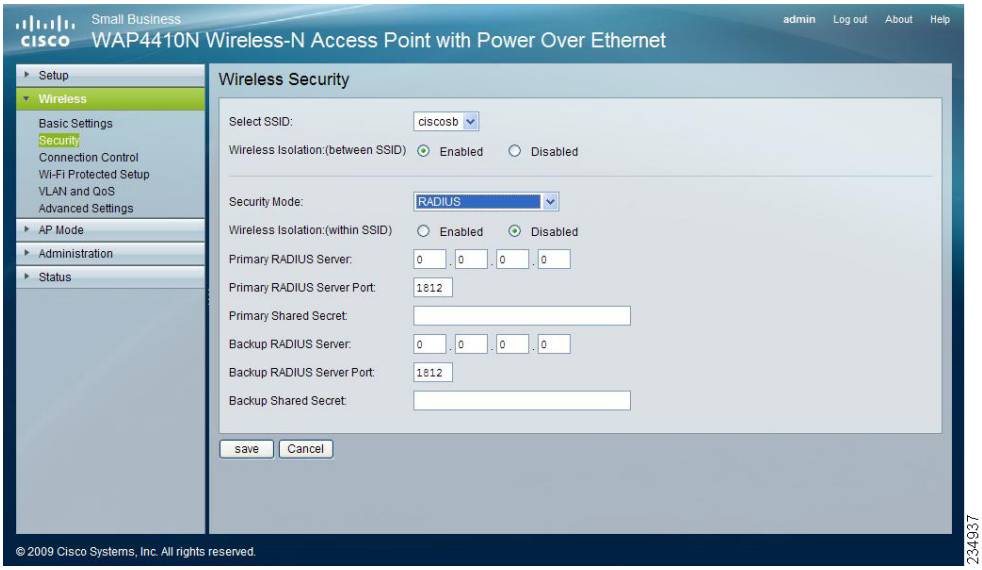
- **Primary/Backup RADIUS Server**—Enter the IP address of the RADIUS server. The Backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the access point and RADIUS server. The backup Radius server is used only if the primary server is unavailable.
- **WPA Algorithms**—WPA offers you two encryption methods, TKIP and AES for data encryption. Select one of these algorithms. The default is **TKIP**.
- **Key Renewal Timeout**—Enter a key renewal timeout period, which instructs the access point how often it should change the encryption keys. The default is **3600** seconds.

STEP 5 Click **Save**.

Configuring RADIUS Security

This option features a RADIUS server for client authentication.

CAUTION Use this mode only when a RADIUS server is connected to the access point.



To enable wireless Remote Authentication Dial-In User Service (RADIUS) security, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 From the Security Mode drop-down menu, select RADIUS.

STEP 3 To enable wireless isolation within the SSID, click **Enabled**.

STEP 4 Provide the following information:

- **Primary/Backup RADIUS Server**—Enter the IP address of the RADIUS server. The Backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the access point and RADIUS server. The backup Radius server is used only if the primary server is unavailable.

STEP 5 Click **Save**.

Configuring WEP Security

This security mode is defined in the original IEEE 802.11. This mode is not recommended now due to its weak security protection. For better security, migrate to WPA or WPA2.

To enable wireless Wired Equivalent Privacy (WEP) security, follow these steps:

STEP 1 Click **Wireless** > **Security**.

STEP 2 From the Security Mode drop-down menu, select WEP.

STEP 3 To enable wireless isolation within the SSID, click **Enabled**.

STEP 4 Provide the following information:

- **Authentication Type**—Choose **Open System** or **Shared Key** as the 802.11 authentication type. The default is **Open System**.
- **Default Transmit Key**—Select the key to be used for data encryption.
- **WEP Encryption**—Select a level of WEP encryption, **64 bits (10 hex digits)** or **128 bits (26 hex digits)**.
- **Passphrase**—To generate WEP keys using a passphrase, then enter the passphrase in the Passphrase field and click **Generate**. The auto-generated keys are not as strong as manual WEP keys.
- **Key 1-4**—To manually create WEP keys, enter these keys in the Key 1, Key 2, Key 3, and Key 4 fields. Each WEP key can consist of the letters "A" through "F" and the numbers "0" through "9.". A key should be 10 characters in length for 64-bit encryption or 26 characters in length for 128-bit encryption.

STEP 5 Click **Save**.

Configuring Connection Control

The Wireless > Connection Control Settings page displays the wireless connection settings.

- "Disabling Connection Control" on page 40
- "Enabling Local Connection Control" on page 41
- "Enabling RADIUS Connection Control" on page 42

Disabling Connection Control

You can use the Wireless > Connection Control Settings page to disable connection control.

To disable wireless connection control for your access point, follow these steps:

STEP 1 Click **Wireless > Connection Control**.

STEP 2 Click **Disabled**.

STEP 3 Click **Save**.

Enabling Local Connection Control

To enable local connection control for your access point, follow these steps:

STEP 1 Click **Wireless > Connection Control**.

STEP 2 Click **Local**.

There are two ways to control the connection (association) of wireless client devices. You can either **prevent** specific devices from connecting to the access point, or you can **allow** only specific client devices to connect to the access point.

The client devices are specified by their MAC addresses. The default is to **allow** only specific client devices.

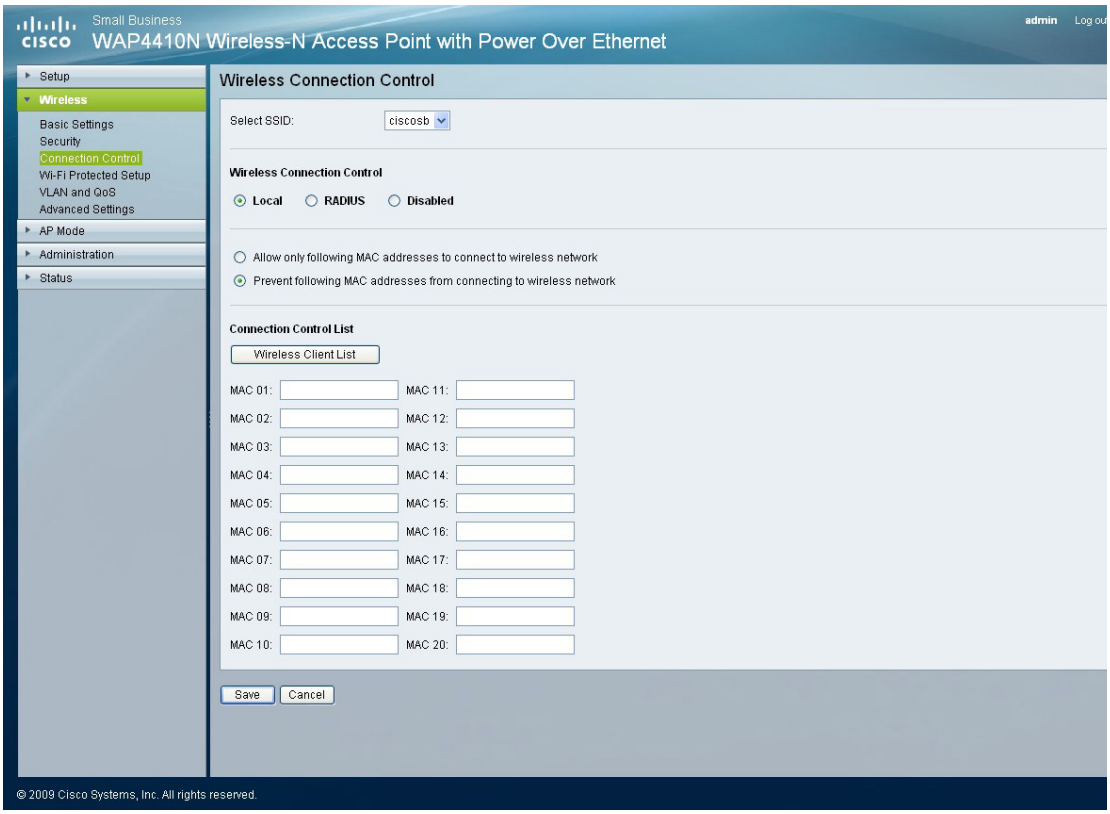
STEP 3 To add a MAC address to the connection control list, click **Wireless Client List**.

In the window that appears, select a MAC address to add to the connection control list.

You can also manually add MAC addresses to the connection control list by entering these addresses in the MAC 01–20 fields.

STEP 4 Click **Save**.

Enabling RADIUS Connection Control



To enable RADIUS connection control for your access point, follow these steps:

STEP 1 Click **Wireless > Connection Control**.

STEP 2 Click **RADIUS**.

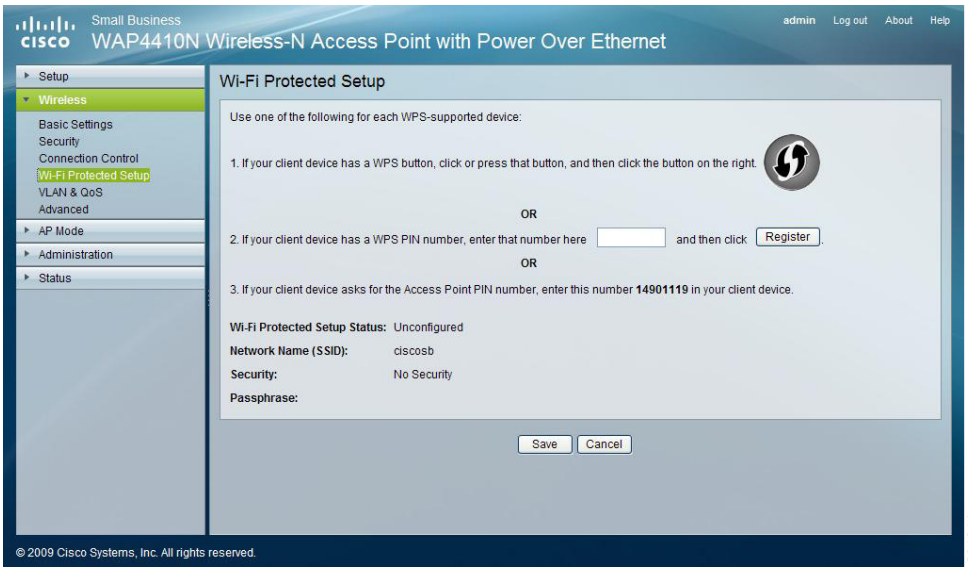
STEP 3 Provide the following information:

- **Primary/Backup RADIUS Server**—Enter the IP address of the RADIUS server. The Backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup RADIUS Server Port**—Enter the port number used by the RADIUS server. The default is 1812. The backup Radius server is used only if the primary server is unavailable.
- **Primary/Backup Shared Secret**—Enter the Shared Secret key used by the access point and RADIUS server. The backup Radius server is used only if the primary server is unavailable.

STEP 4 Click **Save**.

Configuring Wi-Fi Protected Setup

The Wireless > Wi-Fi Protected Setup page allows you to configure the Wi-Fi Protected Setup (WPS) settings for the access point. WPS was designed to help standardize and simplify ways of setting up and configuring security on a wireless network by typing a PIN (numeric code) or pushing a button (Push-Button Configuration, or PBC).



To configure the wireless WPS settings of the access point, follow these steps:

STEP 1 Click **Wireless** > **Wi-Fi Protected Setup**.

STEP 2 Configure the wireless wi-fi settings by doing one of the following actions:

- **Option 1**—Use this method only if the client device has the WPS push button. Press the **WPS** button of the client device and then click the button on the right.
- **Option 2**—Provide the PIN number of the client device. You can find this number in the utility of the device. Enter the number and click **Register**.
- **Option 3**—Enter the PIN number shown on the label at the bottom of the access point into the utility of the client device.

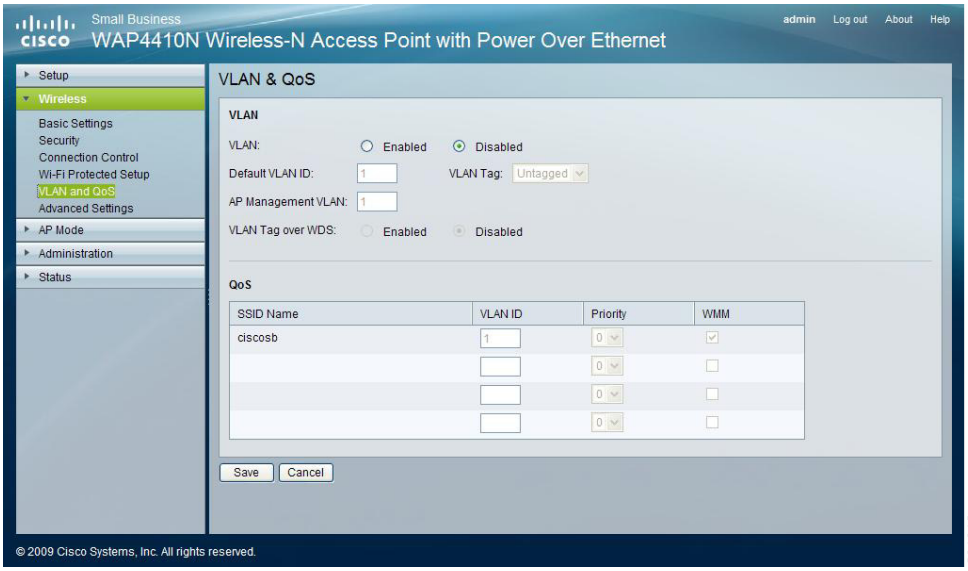
STEP 3 Click **Save**.

Configuring VLAN & QoS

This Wireless > VLAN & QoS page allows you to configure the Qos and VLAN settings for the access point.

The Quality of Service (QoS) feature allows you to specify priorities for different types of traffic.

Lower priority traffic will be slowed down to allow greater throughput or less delay for high priority traffic. The 802.1Q VLAN feature allows traffic from different sources to be segmented. Combined with the multiple SSID feature, this provides a powerful tool to control access to your network.



To configure the wireless VLAN and QoS settings of the access point, follow these steps:

STEP 1 Click **Wireless** > **VLAN & QoS**.

STEP 2 To configure VLAN settings:

NOTE You can enable this feature only if the hubs/switches on your network support the VLAN standard.

a. To enable VLAN, click **Enabled**.

b. Provide the following information:

- **Default VLAN ID**—Enter the default VLAN ID.
- **VLAN Tag**—Select **Tagged** to determine the associated VLAN from the VLAN tag. The default is **Untagged**.
- **AP Management VLAN**—Specify the VLAN ID used for management.
- **VLAN Tag over WDS**—Select **Enabled** or **Disabled** as required.

STEP 3 To configure the QoS settings, enter the following information:

- **VLAN ID**—Enter the ID to assign to the VLAN.
- **Priority**—Select a priority from the list.
- **WMM**—To enable WMM, check the corresponding check box.

  Wi-Fi Multimedia is a QoS feature defined by WiFi Alliance before IEEE 802.11e was finalized. Now it is part of IEEE 802.11e. When it is enabled, it provides four priority queues for different types of traffic. It automatically maps the incoming packets to the appropriate queues based on QoS settings (in IP or layer 2 header). WMM provides the capability to prioritize traffic in your environment. The default in **Enabled**.

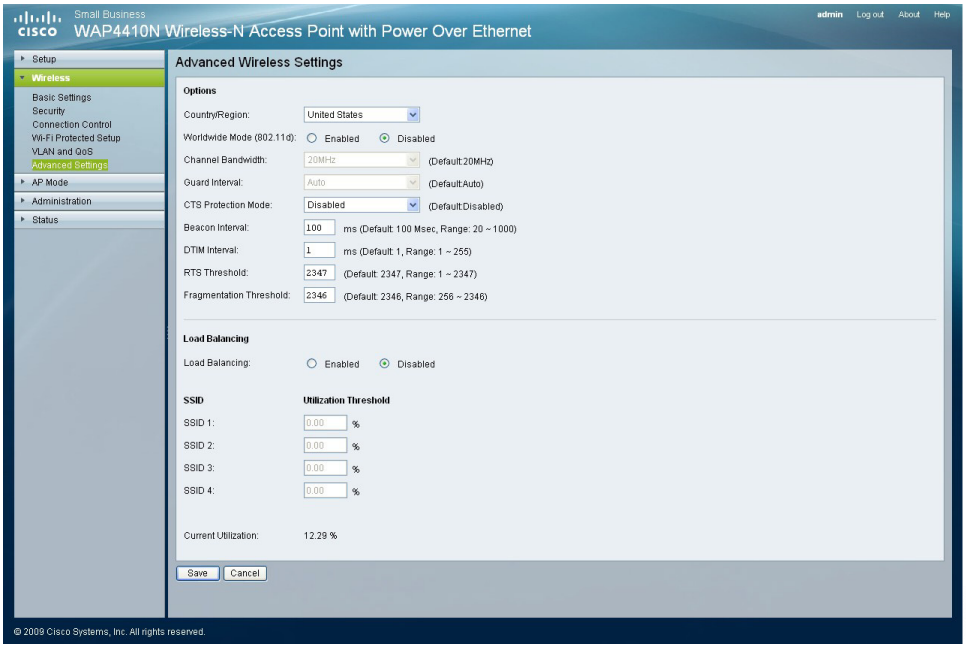
STEP 4 Click **Save**.

Configuring Advanced Settings

The Wireless > Advanced page allows you to configure the advanced and load balancing settings for the access point.

The Wireless-N adopts several new parameters to adjust the channel bandwidth, and guard intervals to improve the data rate dynamically.

We recommend you let your access point automatically adjust the parameters for maximum data throughput.



To configure the wireless advanced settings for the access point, follow these steps:

STEP 1 Click **Wireless** > **Advanced**.

STEP 2 In the Options section, configure the following advanced parameters (some only for Wireless-N) for this access point:

- **Country/Region**—Choose the country for your location from the drop-down list.
- **Worldwide Mode (802.11d)**—Click **Enabled** to enable this mode. Your wireless stations must support this mode for this setting to work.

- **Channel Bandwidth**—Select the channel bandwidth for Wireless-N connections. If you choose **20MHz**, only the 20MHz channel is used. If you choose **40MHz**, Wireless-N connections use the 40MHz channel, but Wireless-B and Wireless-G connections still use the **20MHz** channel. The default is **20MHz**.
- **Guard Interval**—Select a guard interval for Wireless-N connections. The three options are **Auto**, **Short (400ns)** and **Long (800ns)**. The default is **Auto**.
- **CTS Protection Mode**—Keep the default setting, **Auto**, so the access point can use this feature as needed when the Wireless-N/G products are not able to transmit to the access point in an environment with heavy 802.11b traffic. Select **Disabled** if you want to permanently disable this feature.

  This mode boosts the ability of the access point to catch all wireless transmissions, but severely decrease performance.
- **Beacon Interval**—Enter the frequency interval of the beacon (20–1000).

  A beacon is a packet broadcast by the access point to keep the network synchronized. A beacon includes the wireless networks service area, the access point address, the Broadcast destination addresses, a time stamp, Delivery Traffic Indicator Maps, and the Traffic Indicator Message (TIM).

  The default is **100** ms.
- **DTIM Interval**—Enter a Delivery Traffic Indication Message (DTIM) interval (1–255).

  This value indicates how often the access point sends out a DTIM. Lower settings result in more efficient networking, while preventing your computer from dropping into power-saving sleep mode.

  Higher settings allow your computer to enter the sleep mode, thus saving power, but interferes with wireless transmissions.

  The default is **1** ms.
- **RTS Threshold**—Enter an RTS threshold (1–2347).

  This setting determines how large a packet can be before the access point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of **2347**. If you encounter inconsistent data flow, only minor modifications are recommended.
- **Fragmentation Threshold**—Enter the preferred setting between 256 and 2346. Normally, this can be left at the default value of **2346**.

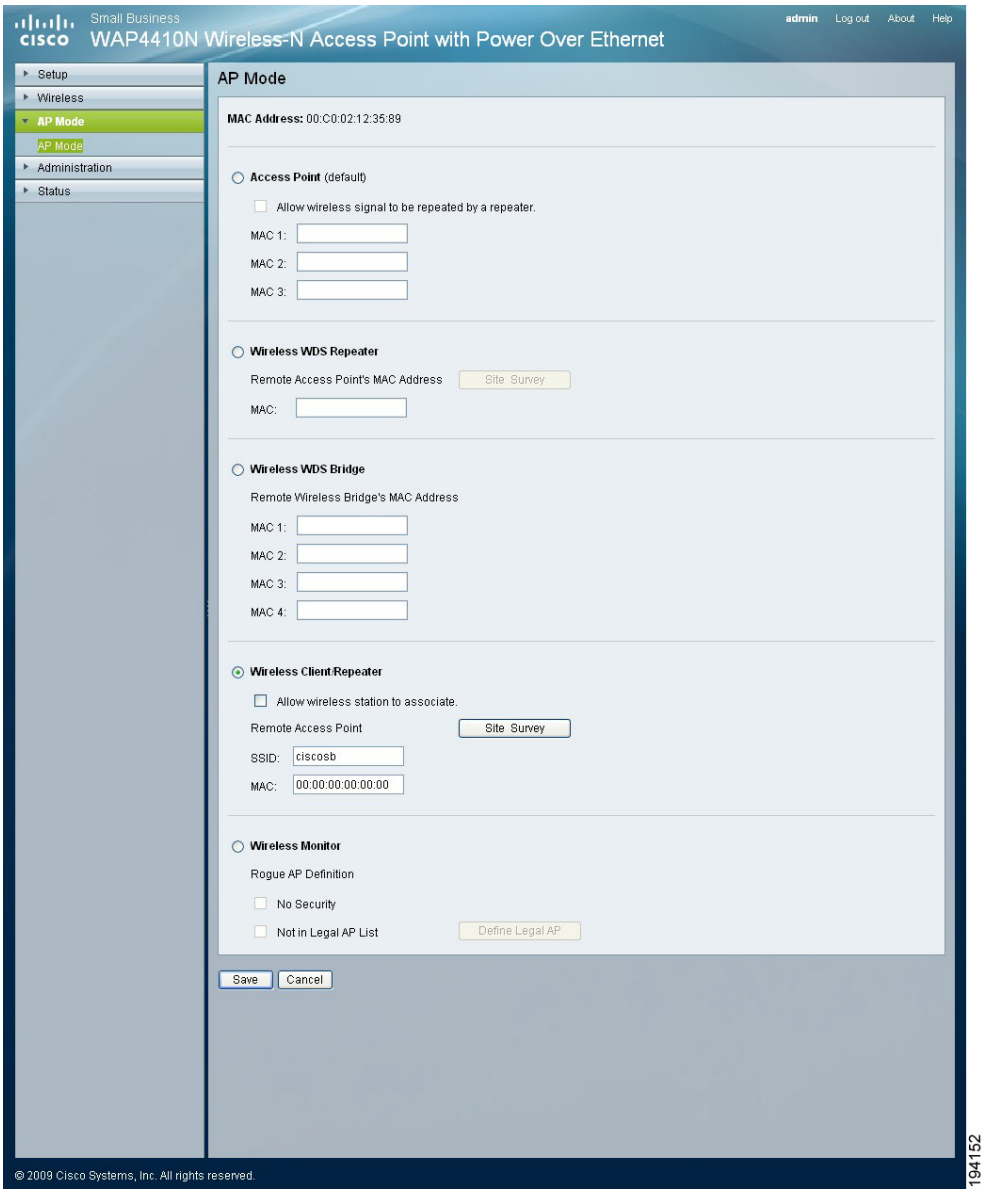
STEP 3 In the Load Balancing section, configure the following advanced parameters for this access point:

- **Load Balancing**—Enable this feature to spread work between two or more access points to get optimal resource utilization, throughput, or response time.
- **Utilization Threshold**—Enter the desired utilization value for the SSID.
- **Current Utilization**—Display the current value of the utilization.

STEP 4 Click **Save**.

Configuring the AP Mode

The AP Mode > AP Mode Settings page displays the AP mode settings for the access point.



To configure the AP mode of the access point, follow these steps:

STEP 1 Click **AP Mode > AP Mode**.

STEP 2 Configure the AP Mode settings.

- **Access point—**Select this option to let the device operate as a normal access point.
  - **Allow Wireless Signal to be repeated by a repeater—**If selected, the device will act as a repeater for another access point. Provide the MAC addresses of the other access points in the fields.
- **Wireless WDS Repeater—**Select this option to let the access point operates as a wireless repeater to extend the radio range of the associated remote access point to overcome any obstacle that blocks radio communication.
  - **Remote Access Point's MAC Address—**Enter the MAC address of the remote access point directly, or click the Site Survey button to select from a list of available access points.
- **Wireless WDS Bridge—**Select this option to let the access point operates as a wireless bridge to perform transparent bridging with other associated wireless bridges, and not allow any wireless client or station to access them.
  - **Remote Wireless Bridge's MAC Address—**Enter the MAC addresses of the other access points in the fields.
- **Wireless Client/Repeater—**Select this option to let the wireless access point operate as a client or repeater access point, sending all traffic received to another access point.
  - **Allow wireless stations to associate—**Enable or disable this setting.
  - **Remote access point—**Enter the MAC address and SSID of the desired access point or click the **Site Survey** button to choose the access point from the available networks.

- **Wireless Monitor**—Allows the access point to detect unauthorized (rogue) access points on your network.
  - **No Security**—Check this check box to identify any access point operating with security disabled as a rogue access point.
  - **Not in Legal AP List**—Check this check box to flag any access point not listed in the Legal AP List as a rouge access point. If you check this check box, you must maintain the Legal AP List.
  - **Define Legal AP**—Click this button to open a sub-screen where you can modify the Legal AP List. This list must contain all known access points. You must keep this list up to date.

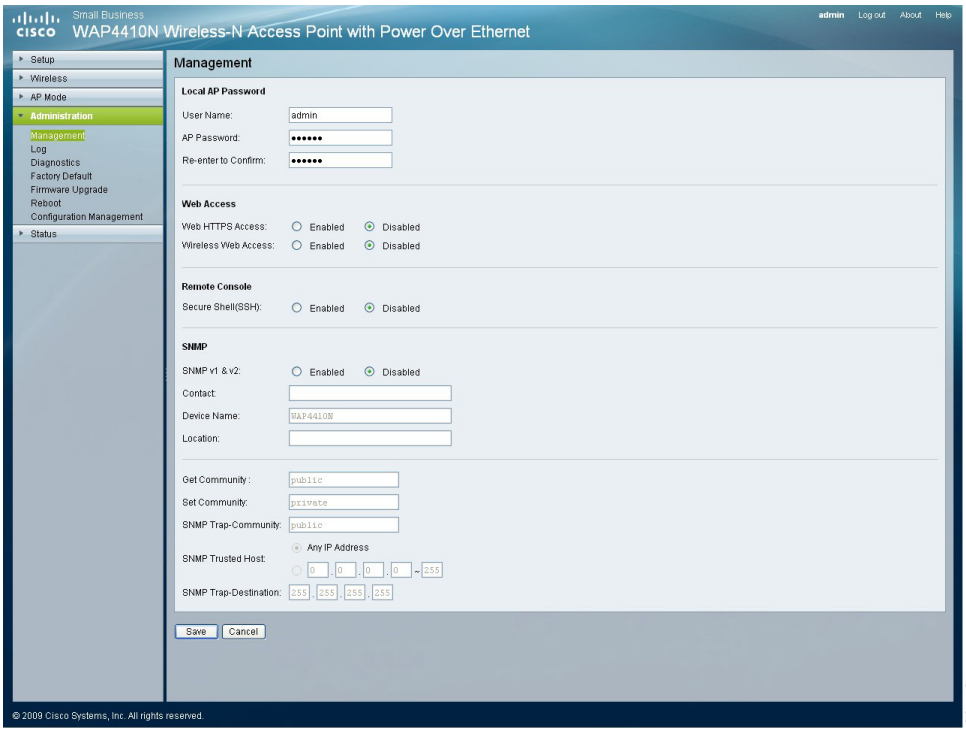
STEP 3 Click **Save**.

Administration

This section describes how to configure the administration settings of the access point:

Configuring Administration Settings

The Administration > Management page allows you to configure the password, Web Access, and SNMP settings. You should change the username/password that controls access to the access point's web-based utility to prevent unauthorized access.



To change the management settings of the access point, follow these steps:

STEP 1 Click **Administration > Management**.

STEP 2 Configure the management settings.

- **Local AP Password**
  - **User Name**—Modify the administrator user name. The default is **admin**.
  - **AP Password**—Modify the administrator password for the access point's web-based utility. The default is **admin**.
  - **Re-enter to confirm**—Confirm the new password by entering it again in this field.

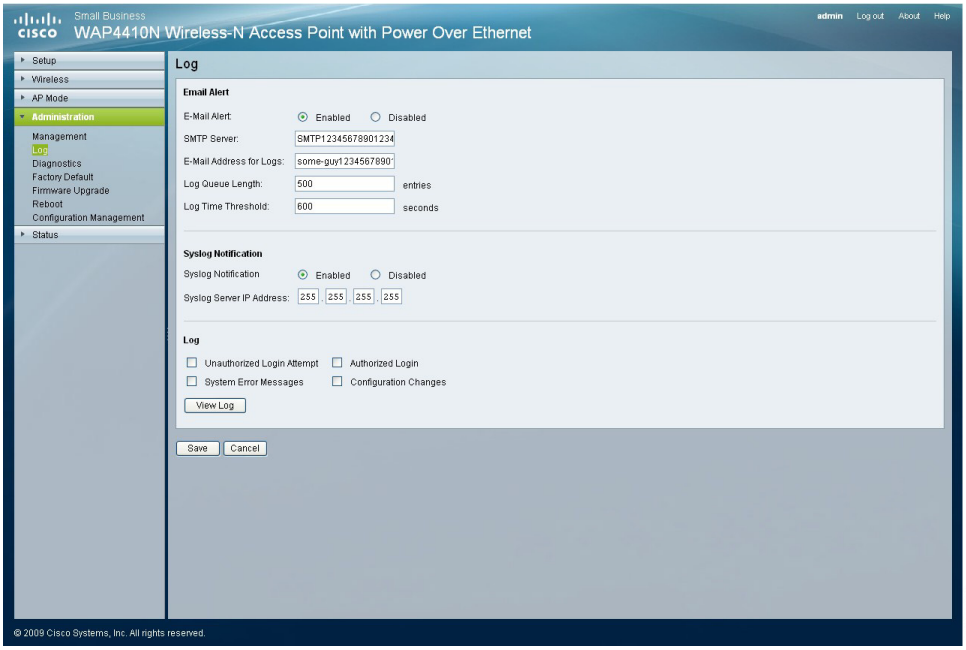
- **Web Access—**Enable HTTPS to increase the security on accessing the web-based utility. Once enabled, users need to use https:// when accessing the Web-based Utility.
  - **Web HTTPS Access—**Enable HTTPS if needed. The default is **Disabled**.
  - **Wireless Web Access—**Allow or deny wireless clients to access web-based utility. The default is **Enabled**.
- **Remote Console—**Enable Secure Shell (SSH) to exchange data over a secure channel between two computers.
  - **Secure Shell (SSH)—**Enable SSH if needed. The default is **Disabled**.
- **SNMP—**Simple Network Management Protocol (SNMP) is a popular network monitoring and management protocol. It provides network administrators with the ability to monitor the status of the access point and receive notification of any critical events as they occur on the access point.

  To enable the SNMP support feature, click **Enabled**. Otherwise, click **Disabled**. The default is **Disabled**.
- **Identification**
  - **Contact—**Enter the name of the contact person, such as a network administrator, for the access point.
  - **Device Name—**Enter the name you want to assign to the access point.
  - **Location—**Enter the location of the access point.
  - **Get Community—**Enter the password that allows read-only access to the access point's SNMP information. The default is **public**.
  - **Set Community—**Enter the password that allows read/write access to the access point's SNMP information. The default is **private**.
  - **SNMP Trap-Community—**Enter the password required by the remote host computer that will receive trap messages or notices sent by the access point.
  - **SNMP Trusted Host—**You can restrict access to the access point's SNMP information by IP address. Enter the IP address in the field provided. If this field is left blank, then access is permitted from any IP address.
  - **SNMP Trap-Destination—**Enter the IP address of the remote host computer that will receive the trap messages.

STEP 3 Click **Save**.

Configuring Administration Log

The Administration > Log page configures the log settings and provides alerts for particular events.



To configure the log settings of the access point, follow these steps:

STEP 1 Click **Administration > Log**.

STEP 2 Configure the log settings.

- **Log**—Allows you to have logs that keep track of the access point's activities.
- **Email Alert**
  - **E-Mail Alert**—If you want the access point to send e-mail alerts in the event of certain attacks, click **Enabled**. The default is **Disabled**.
  - **SMTP Server**—Enter the address or IP address of the Simple Mail Transport Protocol (SMTP) server (incoming mail server).

- **E-Mail Address for Logs**—Enter the e-mail address that will receive logs.
- **Log Queue Length**—Enter the length of the log that will be e-mailed to you. The default is **20** entries.
- **Log Time Threshold**—Enter how often the log will be emailed to you. The default is **600** seconds (10 minutes).

- **Syslog Notification**—Syslog is a standard protocol used to capture information about network activity. The access point supports this protocol and sends its activity logs to an external server. To enable Syslog, click **Enabled**. The default is **Disabled**.
  - **Syslog Server IP Address**—Enter the IP address of the Syslog server. In addition to the standard event log, the access point can send a detailed log to an external Syslog server. The access point's Syslog captures all log activities and includes this information about all data transmissions: every connection source and destination IP address, IP server, and number of bytes transferred.
- **Log**—Select the events that you want the access point to keep a log.
  - **Unauthorized Login Attempt**—If you want to receive alert logs about any unauthorized login attempts, click this check box.
  - **Authorized Login**—If you want to log authorized logins, click this check box.
  - **System Error Messages**—If you want to log system error messages, click this check box.
  - **Configuration Changes**—If you want to log any configuration changes, click the check box.
  - **View Log**—If you want to see the logs, click the button.

STEP 3 Click **Save**.

Diagnosing Access Point Problems

The Administration > Diagnostics page allows you to use the access point to perform a ping. The activity can be useful in solving network problems.

To perform a ping test to help diagnose problems with the access point, follow these steps:

STEP 1 Click **Administration > Diagnostics**.

STEP 2 Set up the ping test:

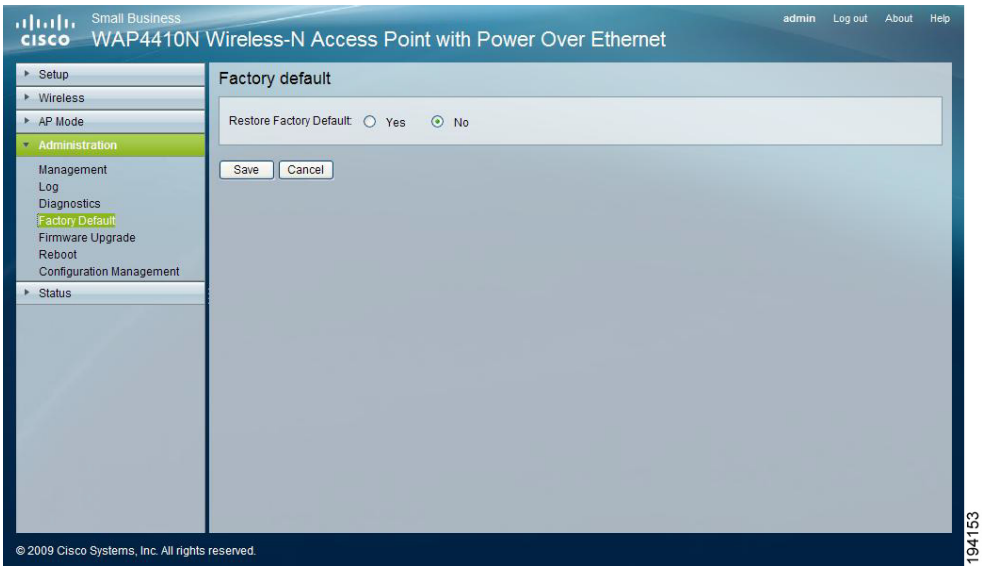
- **IP or URL Address**—Enter the IP address you want to ping. The IP address can be on your network or on the Internet.

NOTE If the address is on the Internet, and no connection currently exists, you could get a timeout error. In that case, wait a few seconds and try again.

- **Packet Size**—Enter the size of the packet.
- **Times to Ping**—Select the times to ping from the list.
- **Start to Ping**—Click this button to start the ping procedure.

Restoring Factory Default Settings

The Administration > Factory Default page allows you to restore the access point's factory default settings.



To restore factory default settings of the access point, follow these steps:

STEP 1 Open the Restore Factory Default page (Administration > Factory Default).

STEP 2 Restore the Factory Default settings.

Restoring Factory Defaults

Note any custom settings before you restore the factory defaults. Once the access point is reset, you will have to re-enter all of your configuration settings.

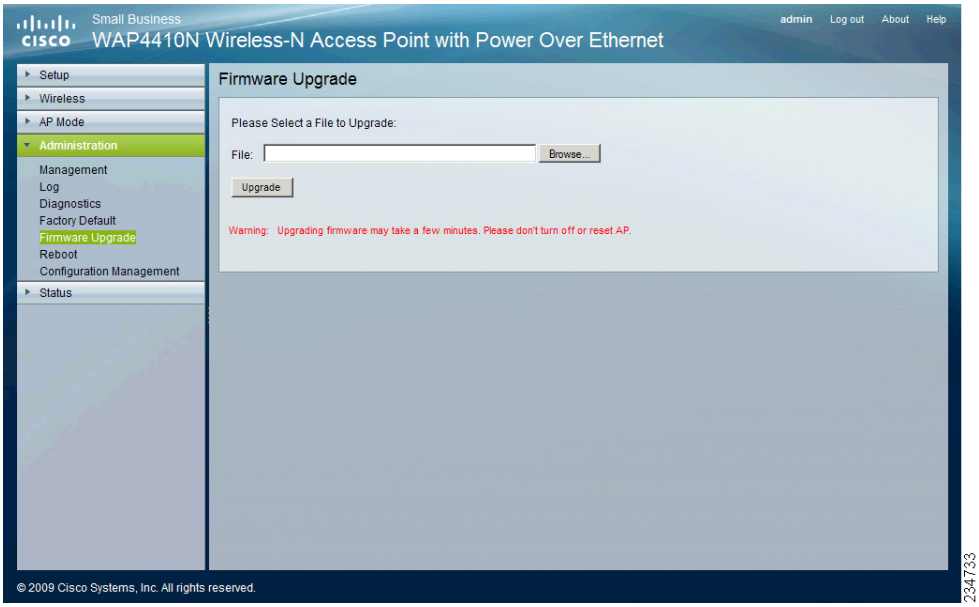
- **Restore Factory Defaults**—To restore the access point's factory default settings, click the **Yes** radio button. Then, click **Save Settings**. Your access point will reboot and come back up with the factory default settings in a few seconds.

Click **Save Settings** to apply your change, or click **Cancel Changes** to cancel your change. Help information is displayed on the right-hand side of the screen.

Upgrading the Firmware

The Administration > Firmware Upgrade page allows you to upgrade the access point's firmware.

CAUTION Do not upgrade the firmware unless you are experiencing problems with the access point or the new firmware has a feature you want to use.



CAUTION Upgrading the firmware deletes all custom settings.

To upgrade the firmware of the access point, follow these steps:

STEP 1 Back up the configuration settings of your access points (see "Managing the Access Point's Configuration" on page 60).

STEP 2 Upgrade the access point's firmware:

a. Download the firmware upgrade file from:

www.cisco.com/en/US/products/ps10052/index.html

b. Extract the firmware upgrade file.

c. Click **Administration > Firmware Upgrade**.

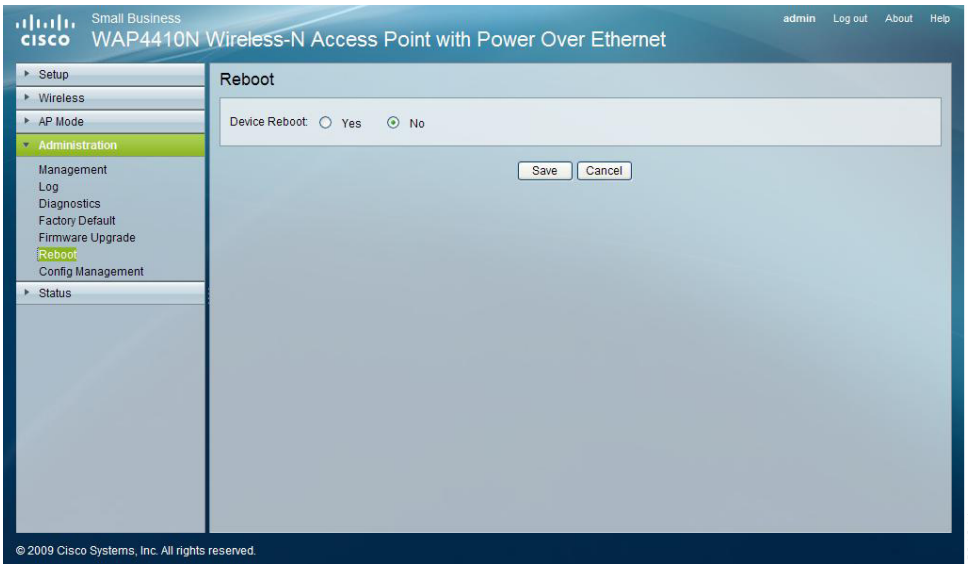
d. In the File field, enter the location of the firmware upgrade file or click the **Browse** button to locate the file.

e. Click **Upgrade** and follow the on-screen instructions.

STEP 3 Re-enter all of your custom configuration settings.

Rebooting the Access Point

The Administration > Reboot page allows you to reboot the access point.



To reboot the access point, follow these steps:

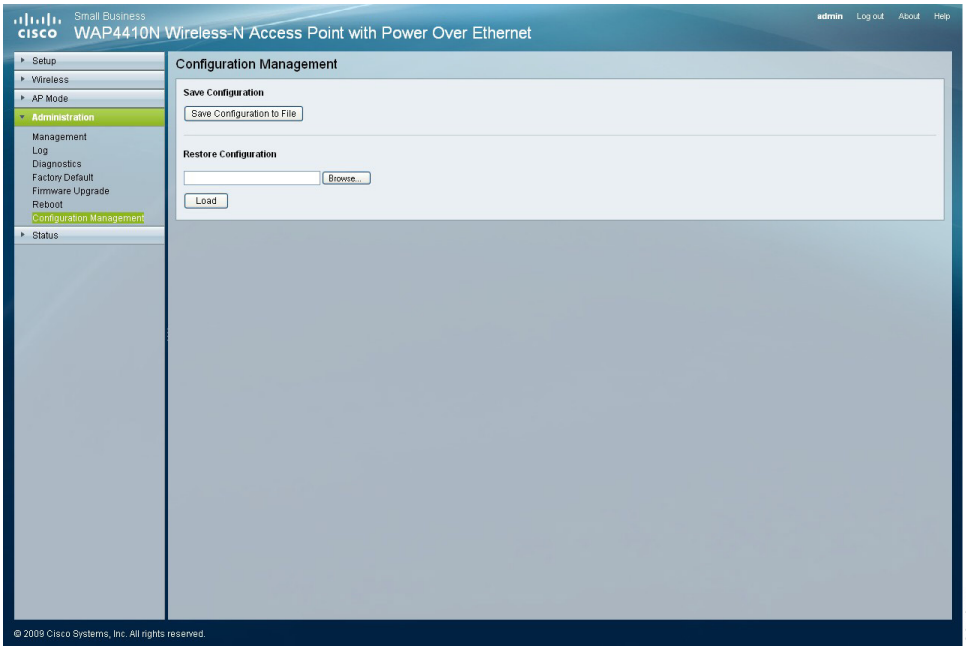
STEP 1 Click **Administration > Reboot**.

STEP 2 In the Device Reboot field, click **Yes**.

STEP 3 Click **Save**.

Managing the Access Point's Configuration

The Administration > Config Management page allows you to create a backup configuration file or upload a configuration file to the access point.



To manage the configuration for the access point, follow these steps:

STEP 1 Click **Administration > Config Management**.

STEP 2 To create a backup configuration file, click **Save Configuration to File** and follow the on-screen instructions.

STEP 3 To restore the configuration of your access point:

a. Make sure that the configuration file for the access point is on your computer.

b. In the **Restore Configuration** field, enter the location of the configuration file or click **Browse** and locate the configuration file.

c. Click **Load**.

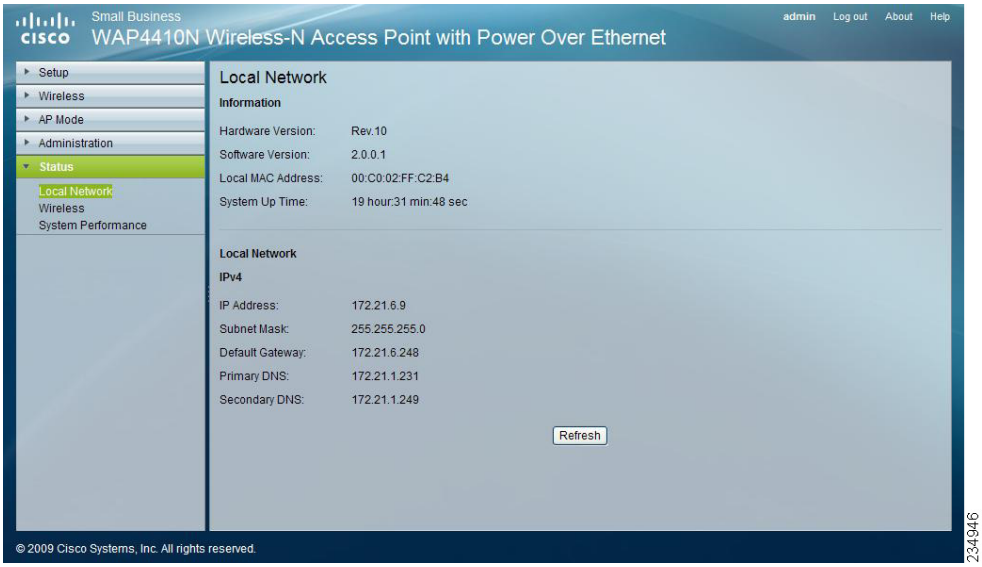
Configuring Status Settings

This section describes how to change the status settings for the access point:

- "Checking Local Network Status" on page 61
- "Checking the Wireless Status" on page 63
- "Checking System Performance" on page 64

Checking Local Network Status

The Status > Local Network page displays the access point's current status information for the local network.



To check local network status, follow these steps:

STEP 1 Click **Status > Local Network**.

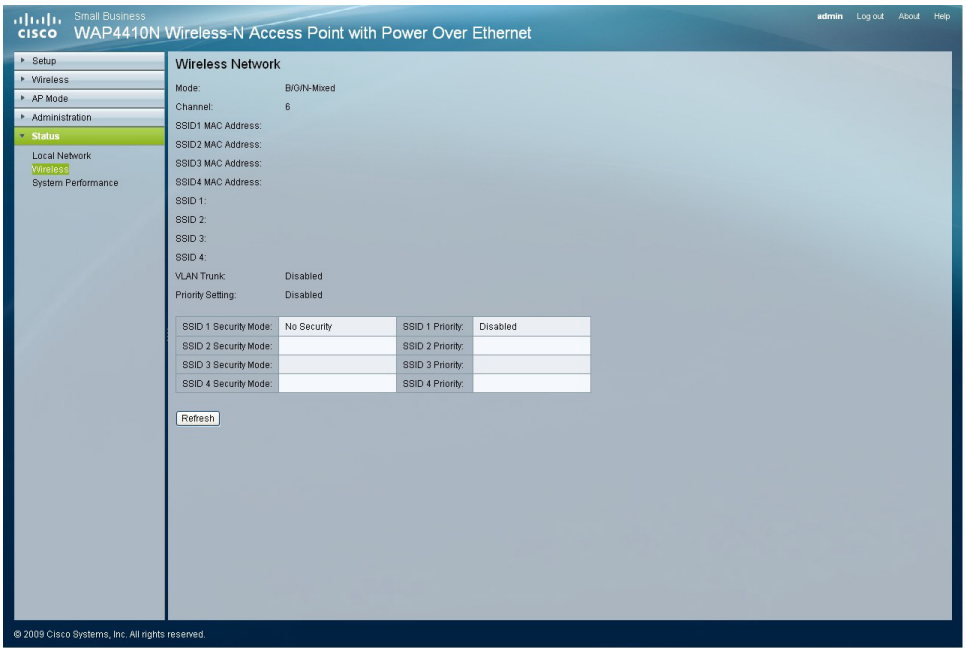
This page displays the status information of your access point:

- **Information**
  - **Hardware Version**—The version of the access point's current hardware.
  - **Software Version**—The version of the access point's current software.
  - **Local MAC Address**—The MAC address of the access point's local network interface.
  - **System Up Time**—The length of time the access point has been running for.
- **Local Network**
  - **IP Address**—The access point's IP address as it appears on your local network.
  - **Subnet Mask**—The access point's subnet mask.

STEP 2 To update the status information, click **Refresh**.

Checking the Wireless Status

The Status > Wireless page displays the access point's current status information for the wireless network.



To check wireless network status of the access point, follow these steps:

STEP 1 Click **Status > Wireless**.

This page displays the status of the wireless network:

- **Mode**—The access point's wireless network mode.
- **Channel**—The access point's channel setting.
- **SSID 1–4 MAC Address**—The MAC address of the access point's wireless interface.
- **SSID 1–4**—The access point's SSID.
- **VLAN Trunk**—The access point's VLAN Trunk status.
- **Priority Setting**—The current priority setting.
- **SSID 1–4 Security Mode**—The security mode of the SSID.
- **SSID 1–4 Priority**—The priority status of the SSID.

STEP 2 To update the wireless status information, click **Refresh**.

Checking System Performance

The Status > System Performance page displays the access point's status information for its current settings and data transmissions.

To check system performance of the access point, follow these steps:

STEP 1 Click Status > Systems Performance.

This page displays the access point's system performance values:

- **Wired**—The statistics for the wired network.
  - **IP Address**—The access point's local IP address.
  - **MAC Address**—The MAC address of the access point's wired interface.
  - **Connection**—The status of the access point's connection for the wired network.
  - **Packets Received**—The number of packets received.

- **Packets Sent**—The number of packets sent.
- **Bytes Received**—The number of bytes received.
- **Bytes Sent**—The number of bytes sent.
- **Error Packets Received**—The number of error packets received.
- **Drop Received Packets**—The number of packets being dropped after they were received.

- **Wireless**—The statistics for the wireless network.
  - **Name**—The wireless network/SSID the statistics refer to.
  - **IP Address**—The access point's local IP address.
  - **MAC Address**—The MAC Address of the access point's wireless interface.
  - **Connection**—The status of the access point's wireless networks.
  - **Packets Received**—The number of packets received for each wireless network.
  - **Packets Sent**—The number of packets sent for each wireless network.
  - **Bytes Received**—The number of bytes received for each wireless network.
  - **Bytes Sent**—The number of bytes sent for each wireless network.
  - **Error Packets Received**—The number of error packets received for each wireless network.
  - **Drop Received Packets**—The number of packets being dropped after they were received.

STEP 2 To update the system performance status information, click **Refresh**.

A

Troubleshooting and Help

This appendix provides solutions to problems that might occur during the installation and operation of the WAP4410N Access Point.

Read the descriptions below to help solve your problems. If you can't find an answer here, check the Cisco.com website at www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html.

Frequently Asked Questions

Q. Can the access point act as my DHCP Server?

No. The access point is nothing more than a wireless hub, and as such cannot be configured to handle DHCP capabilities.

Q. Can I run an application from a remote computer over the wireless network?

This depends on whether or not the application is designed to be used over a network. Consult the application's documentation to determine if it supports operation over a network.

Q. Can I play multiplayer games with other users of the wireless network?

Yes, as long as the game supports multiple players over a LAN (local area network). Refer to the game's documentation for more information.

Q. Can the access point work with a Centrino client?

Yes. However, a Centrino client only supports 20 MHz channels so the maximum throughput with this client will be 130 Mbps. A WPC300N is recommended instead.

Q. What is the IEEE 802.11b standard?

It is one of the IEEE standards for wireless networks. The 802.11b standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11b standard. The 802.11b

standard states a maximum data transfer rate of 11Mbps and an operating frequency of 2.4 GHz.

Q. What is the IEEE 802.11g standard?

It is one of the IEEE standards for wireless networks. The 802.11g standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11g standard. The 802.11g standard states a maximum data transfer rate of 54Mbps and an operating frequency of 2.4GHz.

Q. What is the IEEE 802.11n draft standard?

It is one of the IEEE standards for wireless networks that is being finalized. The 802.11n standard allows wireless networking hardware from different manufacturers to communicate, provided that the hardware complies with the 802.11n standard. The 802.11n standard states a maximum data transfer rate of 600Mbps and an operating frequency of either 2.4GHz or 5 GHz.

Q. What IEEE 802.11b features are supported?

The WAP4410N Access Point supports the following IEEE 802.11 functions:

- CSMA/CA plus Acknowledge protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation
- Power Management

Q. What IEEE 802.11g features are supported?

The WAP4410N Access Point supports the following IEEE 802.11g functions:

- CSMA/CA plus Acknowledge protocol
- OFDM protocol
- Multi-Channel Roaming
- Automatic Rate Selection
- RTS/CTS feature
- Fragmentation

- Power Management

Q. What IPv6 features are supported?

The WAP4410N Access Point supports the following IPv6 functions:

- Path MTU discovery (RFC1981)
- Internet Protocol v6 -IPv6 (RFC2460)
- IPv6 Neighbor Discovery (ND) (RFC2461)
- IPv6 Stateless Address autoconfiguration (RFC2462)
- ICMPv6: Internet Control Message Protocol v6 ICMPv6 (RFC2643)
- IPv6 Address architecture (RFC3513)
- Default address selection (RFC3484)
- Transmission of IPv6 Packets over Ethernet Networks (RFC 2464)
- IPv6 Node - (RFC4294)
- Dual IPv4/IPv6 stack - simultaneous access from IPv4 and IPv6 client at the same time.

The WAP4410N Access Point supports the following IPv6 Applications:

- WEB/SSL
- SNTP
- PING6
- TRACE Route

Q. What is Ad-hoc?

An Ad-hoc wireless LAN is a group of computers, each with a WLAN adapter, connected as an independent wireless LAN. An Ad-hoc wireless LAN is applicable at a departmental scale for a branch or SOHO operation.

Q. What is Infrastructure?

An integrated wireless and wired LAN is called an Infrastructure configuration. Infrastructure is applicable to enterprise scale for wireless access to a central database, or wireless application for mobile workers.

Q. What is roaming?

Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point.

Before using the roaming function, the workstation must make sure that it is set to the same channel number as the access point of the dedicated coverage area.

To achieve true seamless connectivity, the wireless LAN must incorporate a number of different functions. Each node and access point, for example, must always acknowledge receipt of each message. Each node must maintain contact with the wireless network even when not actually transmitting data.

Achieving these functions simultaneously requires a dynamic RF networking technology that links access points and nodes. In such a system, the user's end node undertakes a search for the best possible access to the system. First, it evaluates such factors as signal strength and quality, as well as the message load currently being carried by each access point and the distance of each access point to the wired backbone. Based on that information, the node next selects the right access point and registers its address.

Communications between end node and host computer can then be transmitted up and down the backbone.

As the user moves on, the end node's RF transmitter regularly checks the system to determine whether it is in touch with the original access point or whether it should seek a new one. When a node no longer receives acknowledgment from its original access point, it undertakes a new search. Upon finding a new access point, it then re-registers, and the communication process continues.

Q. What is the ISM band?

The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band.

Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high speed wireless capabilities in the hands of users around the globe.

Q. What is Spread Spectrum?

Spread Spectrum technology is a wideband radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. It is designed to trade off bandwidth efficiency for reliability, integrity, and security.

In other words, more bandwidth is consumed than in the case of narrowband transmission, but the trade-off produces a signal that is, in effect, louder and thus easier to detect, provided that the receiver knows the parameters of the spread-spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise.

There are two main alternatives, Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS).

Q. What is DSSS? What is FHSS? And what are their differences?

Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern that is known to both transmitter and receiver.

Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise. Direct Sequence Spread Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code).

The longer the chip, the greater the probability that the original data can be recovered. Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission.

To an unintended receiver, DSSS appears as low power wideband noise and is rejected (ignored) by most narrowband receivers.

Q. Would the information be intercepted while transmitting on air?

WLAN features two-fold protection in security. On the hardware side, as with Direct Sequence Spread Spectrum technology, it has the inherent security feature of scrambling. On the software side, the WLAN series offers a variety of wireless security methods to enhance security and access control. Users can set it up depending upon their needs.

Q. Can Cisco wireless products support file and printer sharing?

Cisco wireless products perform the same function as LAN products. Therefore, Cisco wireless products can work with NetWare, Windows NT/2000, or other LAN operating systems to support printer or file sharing.

Q. What is WEP?

WEP is Wired Equivalent Privacy, a data privacy mechanism based on a 40-bit shared-key algorithm, as described in the IEEE 802.11 standard.

Q. What is a MAC Address?

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP addresses, which can change every time a computer logs on to the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

Q. How do I avoid interference?

Using multiple access points on the same channel and in close proximity to one another will generate interference. When employing multiple access points, make sure to operate each one on a different channel (frequency).

Q. How do I reset the access point?

Press the Reset button on the back of the access point for about ten seconds. This resets the unit to its default settings.

Q. How do I resolve issues with signal loss?

There is no way to know the exact range of your wireless network without testing. Every obstacle placed between an access point and wireless computer will create signal loss. Leaded glass, metal, concrete floors, water, and walls will inhibit the signal and reduce range. Start with your access point and your wireless computer in the same room and move it away in small increments to determine the maximum range in your environment.

You may also try using different channels, as this may eliminate interference affecting only one channel. Also, open the access point's web-based utility, click **Wireless** > **Advanced Wireless**, and make sure the output power is set to 100%.

Q. Does the access point function as a firewall?

No. The access point is only a bridge from wired Ethernet to wireless clients.

Q. I have excellent signal strength, but I cannot see my network.

Wireless security, such as WEP or WPA, is probably enabled on the access point, but not on your wireless adapter (or vice versa). Verify that the same wireless security settings are being used on all devices in your wireless network.

Q. What is the maximum number of users the access point can handle?

No more than 63, but this depends on the volume of data and may be fewer if many users create a large amount of network traffic.

Q. How do I configure multiple WAP4410N access points with the same configuration?

STEP 1 Configure one access point and then save the configuration file through its web page.

STEP 2 Using a text editor, change the command "`secret_shown=1`" to "`secret_shown=0`" in the configuration file, and then save the file.

STEP 3 Restore the file to the access point through its web page and save the configuration, naming it `AP_Config.cfg`.

At this point, all keys and passwords are shown in clear text.

STEP 4 Restore the `AP_config.cfg` file on other access point's through their web pages one by one.

Windows Help

Almost all wireless products require Microsoft Windows. Windows is the most used operating system in the world and comes with many features that help make networking easier. These features can be accessed through Windows Help and are described in this appendix.

TCP/IP

Before a computer can communicate with the access point, TCP/IP must be enabled. TCP/IP is a set of instructions, or protocol, all PCs follow to communicate over a network. This is true for wireless networks as well. Your PCs will not be able to utilize wireless networking without having TCP/IP enabled. Windows Help provides complete instructions on enabling TCP/IP.

Shared Resources

If you wish to share printers, folder, or files over your network, Windows Help provides complete instructions on utilizing shared resources.

Network Neighborhood/My Network Places

Other PCs on your network will appear under Network Neighborhood or My Network Places (depending upon the version of Windows you're running). Windows Help provides complete instructions on adding PCs to your network.

B

Wireless Security

This appendix lists safety precautions that you should keep in mind when setting up or using your wireless network.

Security Precautions

The following is a list of security precautions to take to protect your wireless network:

- Change the default SSID.
- Disable SSID broadcasting.
- Change the default password for the Administrator account.
- Change the SSID periodically.
- Use the highest encryption algorithm possible.

  Use WPA if it is available.

  NOTE Using the highest encryption algorithm possible can reduce the performance of your network.

- Change the WEP encryption keys periodically.

Protecting Your Network

Wireless networks are easy to find. Hackers know that to join a wireless network, wireless networking products first listen for "beacon messages." These messages can be easily decrypted and contain much of the network's information, such as the network's SSID (Service Set Identifier).

Here are steps you can take to protect your network:

- **Change the administrator's password regularly.**

  Every wireless networking device stores network settings (for example, SSID and WEP keys) in its firmware.

  Your network administrator is the only person who can change network settings. If a hacker gets a hold of the administrator's password, the hacker, too, can change those settings. So, make it harder for a hacker to get that information. Change the administrator's password regularly.

- **Protecting your SSID.**

  Do the following to protect your SSID:

  - Disable SSID broadcasting.

    Most wireless networking devices give you the option of broadcasting the SSID. While this option may be more convenient, it allows anyone to log into your wireless network. This includes hackers. So, don't broadcast the SSID.

  - Make the SSID unique.

    Wireless networking products come with a default SSID set by the factory. Hackers know these defaults and can check them against your network. Change your SSID to something unique and not something related to your company or the networking products you use.

  - Change the SSID often.

    Change your SSID regularly so that hackers who gain access to your wireless network will have to start from the beginning in trying to break in.

- **MAC Addresses.**

  Enable MAC address filtering. MAC address filtering allows you to provide access to only those wireless nodes with certain MAC addresses. This makes it harder for a hacker to access your network with a random MAC address.

- **WEP Encryption.**

  WEP is often looked upon as a cure-all for wireless security concerns. This is overstating WEP's ability. Again, this can only provide enough security to make a hacker's job more difficult.

  There are several ways that WEP can be maximized:

  - Use the highest level of encryption possible.
  - Use "Shared Key" authentication.
  - Change your WEP key regularly.

- **WPA/WPA2 Personal.**

  The WPA-Personal and WPA2-Personal methods offer two encryption methods, TKIP and AES, with dynamic encryption keys.

- **WPA /WPA2 Enterprise.**

  The WPA-Enterprise and WPA2-Enterprise option requires that your network has a RADIUS server for authentication.

  A network encrypted with WPA/WPA2 is more secure than a network encrypted with WEP, because WPA/WPA2 uses dynamic key encryption. To protect the information as it passes over the airwaves, you should enable the highest protection level.

  Implementing encryption may have a negative impact on your network's performance, but if you are transmitting sensitive data over your network, encryption should be used.

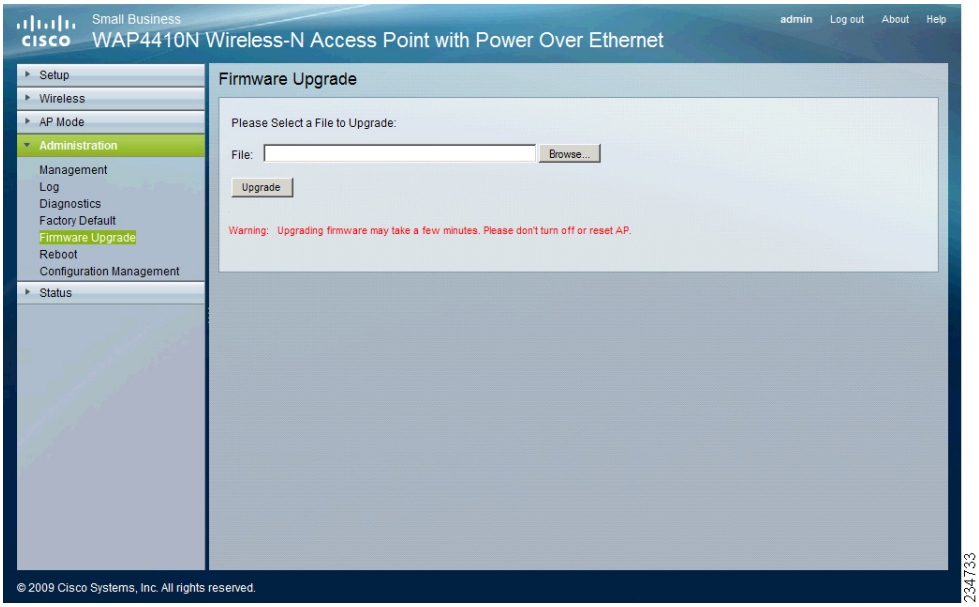
CAUTION: Always remember that each device in your wireless network *must* use the same encryption method and encryption key or your wireless network will not function properly.

C

Upgrading Firmware

The Administration > Firmware Upgrade page allows you to upgrade the access point's firmware.

CAUTION Do not upgrade the firmware unless you are experiencing problems with the access point or the new firmware has a feature you want to use.



CAUTION Upgrading the firmware deletes all custom settings.

To upgrade the firmware of the access point, follow these steps:

STEP 1 Back up the configuration settings of your access points (see "Managing the Access Point's Configuration" on page 60).

STEP 2 Upgrade the access point's firmware:

a. Download the firmware upgrade file from:

www.cisco.com/en/US/products/ps10052/index.html

b. Extract the firmware upgrade file.

c. Click **Administration > Firmware Upgrade**.

d. In the File field, enter the location of the firmware upgrade file or click the **Browse** button to locate the file.

e. Click **Upgrade** and follow the on-screen instructions.

STEP 3 Re-enter all of your custom configuration settings.

D

Specifications

This appendix details the specifications of the Cisco WAP4410N Wireless-N Access Point with Power Over Ethernet.

WAP4410N Specifications

Model	WAP4410N
Standards	Draft IEEE802.11n, IEEE802.11g, IEEE802.11b, IEEE802.3, IEEE802.3u, IEEE802.3af (Power Over Ethernet), 802.1x (Security Authentication), 802.11i Security WPA/WPA2, WMM
Ports	Ethernet, Power
Buttons	Reset
Cabling Type	UTP Cat 5e or higher
LEDs	Power, Ethernet, Wireless, POE
Operating System	Linux
Web UI	Built in Web UI for Easy browser-based configuration (HTTP/HTTPS)
SNMP Version	Versions 1 and 2c
Event Logging	Email logging, Remote Syslog
Web F/W Upgrade	Firmware upgradeable through web-browser
Diagnostics and Flash	Flash, RAM, LAN, WLAN
DHCP	DHCP Client
HTTP Redirect	Redirects initial user access to an external Web Server to display company logo or network usage policy
IPv6 Host	Support for management and control of access point over IPv6. Supports RFC2460 (IPv6 protocol) and RFC4294 (IPv6 Node Requirements)

WAP4410N Specifications (Continued)

Multiple BSSID	Supports up to 4 BSSIDs allowing creating of multiple virtual access points
VLANs	Supports 802.1q - up to 4 VLANs
SSID to VLAN mapping	Supports mapping of SSIDs to VLANs to securely separate workgroups across wireless and wired domains
802.1x Supplicant	Supports 802.1x Supplicant on the Ethernet port to allow the AP to authenticate itself to the network
Spanning Tree	Supports 802.1d Spanning Tree protocol to prevent loops when using WDS links as redundant links in a distribution system
Operating Modes	Access Point Mode, point-to-point Bridge Mode, point-to-multipoint Bridge Mode, Repeater Mode, Wireless Client Mode
Load Balancing	This capability allows the bandwidth control with user defined CPU usage ratio
Auto-channel selection	On boot up, the AP selects the least congested channel
802.11d	With 802.11d Regulatory Domain support, the AP provides radio channel settings for client devices facilitating easy client access as they move across regulatory domains
WEP/WPA/WPA2	WEP 64bit/128bit, WPA-TKIP, WPA2-AES, WPA-Enterprise, and WPA2-Enterprise
Access Control	Wireless Connection Control: MAC-Based
SSID Broadcast	SSID Broadcast Enable/Disable
Client Isolation	Supports wireless client isolation between SSIDs
802.1x	Wireless clients can be authenticated through IEEE 802.1x
802.1x Supplicant	Supports 802.1x Supplicant on the Ethernet port to allow the AP to authenticate itself to the network
Radius Server	Up to 2 Radius Servers can be configured for redundancy purposes
WPS	Supports WPS (WiFi Protected Setup), which is a WIFI Alliance specification for simple and secure setup of a wireless network.

WAP4410N Specifications (Continued)

Rogue AP Detection	New access points detected, which have not been categorized as known, are logged as rogue access points. This allows the administrator to control unapproved devices in the network.
QoS	4 queues, 802.1p VLAN priority, WMM Wireless priority, Mapping of 802.1p priority to WMM priority to maintain end-to-end QoS
Spec/Modulation	Radio and Modulation Type: 802.11b/DSSS, 11g/OFDM, 11n/MIMO-OFDM
Channels	Operating Channels: 11 North America, 13 Most of Europe (ETSI and Japan)
Internal Antenna	None
External Antennas	3 (omni-directional)
Transmit Power	Transmit Power at Normal Temp Range for FCC: 11b - 16 dBm@1TX, 19 dBm@2TX, 20.5dbm@3TX; 11g - 13 dBm@1TX, 16 dBm@2TX, 19dbm@3TX 11n - 20 dBm@MCSO~4/8~12, 18dBm@MCS5/13, 14dBm@MCS6/14, 12dBm@MCS7/15 Transmit Power at Normal Temp Range for ETSI: 11b/g/n: 18.5dBm
Antenna Gain in dBi	2
Receiver Sensitivity	11.n: 300Mbps@ -69dBm, 11.g: 54Mbps@ -73dBm, 11.b: 11Mbps@ -88dBm
Device Dimensions	6.69X6.69X1.60 inches (170X170X40.7mm) 0.86 lbs. (0.39 kg)
Power	12V 1A DC input, and IEEE802.3af Compliant PoE. Maximum power draw is 10.1 Watts.
Certification	CC, CE, IC
Operating Temperature	32°F to 104°F (0°C to 40°C)
Storage Temperature	-4°F to 158°F (-20°C to 70°C)
Operating Humidity	10% to 85% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing

E

Where to Go From Here

Cisco provides a wide range of resources to help you and your customer obtain the full benefits of the Cisco WAP4410N Wireless-N Access Point with Power Over Ethernet.

Product Resources

Resource	Location
Technical Documentation	www.cisco.com/en/US/products/ps10047/tsd_products_support_series_home.html
Firmware Downloads	www.cisco.com/en/US/products/ps10052/index.html
Customer Support	www.cisco.com/en/US/support/tsd_cisco_small_business_support_center_contacts.html
Warranty and End User License Agreement	www.cisco.com/go/warranty
Open Source License Notices	www.cisco.com/go/osln
Regulatory Compliance and Safety Information	www.cisco.com/en/US/products/ps10047/tsd_products_support_series_home.html
Cisco Partner Central site for Small Business	www.cisco.com/web/partners/sell/smb

Related Documentation

For hardware setup for the Cisco WAP4410N access point, see the *Cisco Small Business Model WAP4410N Wireless-N Access Point with Power Over Ethernet Quick Start Guide*.